ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

Ғаниев С. К.,
Каримов М. М.,
Ташев К. А.

АХБОРОТ ХАВФСИЗЛИГИ

Ахборот-коммуникацион тизимлар хавфсизлиги

Олий ўқув юрт талабалари учун мўлжалланган

МУНДАРИЖА

МУҚАДДИМА

Илдам қадамлар билан ривожланаётган компьютер ахборот технологиялари ҳаётимизда сезиларли ўзгаришларга сабаб бўлмоқда. "Ахборот" тушунчаси сотиб олиш, сотиш, бирор нарсага алмашиш ва ҳ. мумкин бўлган махсус товарни белгилашда тез-тез ишлатила бошланди. Бунда ахборотнинг нархи кўпинча у жойлашган компьютер тизими нархидан юз ва минг марта юқори бўлади. Демак, ахборотни рухсатсиз фойдаланишдан, атайин ўзгартиришдан, йўқ қилишдан ва бошқа жиноий ҳаракатлардан ҳимоялаш зарурияти-нинг пайдо бўлиши табиийдир.

Ахборотни ҳимоялаш муаммоси компьютер тизимлари ва тармоқлари соҳасида фаолият кўрсатувчи мутахассислар ҳамда замонавий компьютер воситаларидан фойдаланувчилар эътиборини жалб этмоқда. Айни пайтда компьютер фани ва амалиётининг ушбу долзарб муаммоси Давлат тилида ёзилган илмий-техник ва ўқув адабиётларда етарлича ўз аксини топмаган.

Ўқувчи эътиборига ҳавола этилаётган китоб ахборот-коммуникацион тизимлар хавфсизлигига бағишланган ва 13 та бобдан иборат.

Китобнинг *биринчи бобида* ахборот хавфсизлигининг ҳозирги ҳолатига баҳо берилади. Компьютер жиноятчилиги таҳлил этилиб, тармоқ ахборотига бўладиган намунавий хужум усуллари келтирилади ҳамда ахборот хавфсизлигини бузувчининг модели тавсифланади.

Китобнинг *иккинчи бобида* Internet тармоқнинг асосий ахборот хизматалари тавсифланади. Internet да электрон бизнес ва электрон тижоратнинг асосий моделлари тахлилланади. Электрон савдо ва Internet – хизматларнинг асосий турлари тавсифланади. Электрон бизнес тизими хавфсизлигининг муаммолари кўрилади.

Китобнинг *учинчи бобида* ахборот хавфсизлигининг асосий тушунчалари кўрилади, хавфсизликни таъминлашнинг амалда текширилган принциплари ҳамда хавфсизлик сиёсатини яратиш жараёни тавсифланади. Ахборот-коммуникацион тизимлар ва тармоқлар хавфсизлигига қўйиладиган талаблар келтирилади. Ахборот хавфсизлигини таъминловчи чоралар хусусида сўз юритилади.

Китобнинг *тўртинчи боби* ахборот хавфсизлигининг ҳуқуқий ва ташкилий таъминотига бағишланган. Хавфсизликнинг халқаро ва миллий ҳуқуқий меъёрлари хусусида сўз юритилади.

Китобнинг *бешинчи боби* ахборотни ҳимоялашнинг криптографик усулларига бағишланган бўлиб, маълумотларни шифрлашнинг блокли симметрик алгоритмлари, жумладан, АҚШнинг янги стандарти AES тахлил этилади. Замонавий асимметрик криптотизимлар муҳокама этилади. Хэшлаш функцияларининг асосий хусусиятлари ва ишлатилиш соҳалари аниқланади. Рақамли имзони генерациялаш ва текшириш муолажалари кўрилади. Калитларни бошқариш – калитларни тақсимлаш жараёнига алоҳида эътибор қилинади.

Китобнинг *олтинчи бобида* тизимнинг фойдаланувчилар билан ўзаро алоқасидаги асосий жараёнлар – фойдаланувчи ҳаракатини аутентификациялаш, авторизациялаш ва маъмурлаш тушунтирилади. Кўп мартали ва бир мартали пароллар, ҳамда рақамли сертификатлар асосидаги аутентификациялаш хусусиятлари тахлил этилади. Фойдаланувчини идентификациялаш ва аутентификациялашнинг намунавий схемалари кўрилади. Симметрик ва асимметрик криптоалгоритмларга асосланган қатъий аутентификациялашга алоҳида эътибор берилади. Аутентифкациялашнинг Kerberos протоколи муҳокама этилади. Биометрик идентификациялаш ва аутентификациялаш воситалари тавсифланади.

Китобнинг *еттинчи бобида* тармоқлараро экранларнинг функциялари таҳлил этилиб, уларнинг OSI моделининг турли сатхларида ишлаши хусусиятлари муҳокама қилинади. Тармоқларо экранлар асосида тармоқни ҳимоялаш схемалари тавсифланади. Шахсий ва тақсимланган тармоқ экранларининг ишлатилиши кўрилади.

Китобнинг *саккизинчи бобида* ҳимояланган виртуал хусусий тармоқларни куриш концепцияси кўрилади ва уларнинг асосий хусусияти – туннеллаш шархланади. Виртуал ҳимояланган каналларни қуриш вариантлари таҳлилланади. Ҳимояланган виртула хусусий тармоқларнинг қатор аломатлари бўйича туркумланиши кўрилади. VPN технологиянинг корпоратив ахборот тизимлари ва тармоқларида қўлланилишининг техник ва

иқтисодий афзалликлари кўрсатилади. OSI очиқ тизимлар ўзаро алоқа эталон моделининг канал ва сеанс сатҳларида ҳимояланган виртуал каналлар қурилишининг муаммолари муҳокама этилади. IPSec протоколлар стекининг архитектураси кўрилиб, уларнинг ҳимояланган хусусий тармоқлар қуришда ишлаштилиши кўрилади.

Китобнинг *тўққизини бобида* очиқ калитларни бошқариш инфратузилмаси PKI кўрилади. Очиқ калитларнинг рақамли сертификатларини ишлатиш зарурияти асосланади. PKI нинг ишлаш принциплари муҳокама этилади. Сертификациялашнинг базавий моделлари, PKI нинг мантиқий тузилмаси ва компонентлари келтирилади.

Китобнинг *ўнинчи боби* ахборот хавфсизлигини адаптив бошқаришнинг долзарб муаммоларига бағишланган. Корпоратив тармоқ хавфсизлигини адаптив бошқариш концепцияси тавсифланади. Ҳимояланишни тахлиллашнинг технологиялари ва воситалари батафсил муҳокама этилади. Тармоқ ахборотини тахлиллаш усуллари, хужумларни аниқлаш тизимларининг компонентлари ва архитектураси кўрилади. Компьютер вирусларидан ҳимояланишнинг долзарб муаммолари ҳам ушбу бобдан ўрин олган. Компьютер вирусларининг туркумланиши келтирилади, вирус ҳаёт цикли босқичлари тахлилланади ва вирусларнинг ва бошқа зарар келтирувчи дастурларнинг асосий тарқалиш каналлари кўрилади. Вирусга қарши дастурларнинг асосийлари муҳокама этилади. Вирусга қарши ҳимоя тизимини қуриш масаласи кўрилади.

Китобнинг *ўн биринчи боби* маълумотларни узатиш тармоғида ахборотни ҳимоялаш муаммосига бағишланган. Маълумотларни узатиш тармоғи компонентларига ва архитектурасига реал таъсир этувчи функционал, архитектуравий ва бошқариш (маъмурий) талаблар кўрилади. Алоқа каналларида маълумотларни ҳимоялаш усуллари муҳокама этилади.

Китобнинг *ўн иккинчи боби* симсиз алоқа тизимларида ахборот ҳимоясининг долзарб масалаларига бағишланган. Симсиз тармоқ концепцияси ва тузилмаси кўрилади. Симсиз тармоқ хавфсизлигига тахдидлар батафсил тахлил этилиб, симсиз тармоқ хавфсизлиги протоколлари муҳокама

этилади. Симсиз қурилмалар хавфсизлиги муаммолари ҳам ушбу бобдан ўрин олган.

Китобнинг *ўн учинчи боби* тармоқ хавфсизлиги воситаларини бошқариш усулларига бағишланган. Ахборот тизимларини бошқаришнинг кенг тарқалган методологияси ITIL тавсифланади. Корхона миқёсида ахборотни ҳимоялаш тизимини бошқариш масаласи таърифланади. Хавфсизликни марказлаштирилган бошқаришнинг глобал ва локал хавфсизлик сиёсатига асосланган истиқболли архитектурасига алоҳида эътибор берилади. Ахборот тизимлари хавфсизлигининг аудити ва мониторинги кўрилади. Хавф-хатарларни тахлиллаш ва бошқариш муаммоси, ҳамда тармоқ хавфсизлик тизимини қуриш методологияси тавсифланади.

Қўлланмани тайёрлашда яқиндан ёрдам берган (VII ва XI боблар) техника фанлари номзоди А.А. Ғаниевга, тақризчиларга ҳамда ўқув қўлланма ҳақидаги барча фикр мулоҳазалари учун ҳурматли китобхонларга муаллифлар ўз миннатдорчиликларини изҳор этадилар.

Муаллифлар

I боб. АХБОРОТ ХАВФСИЗЛИГИГА ТАҲДИДЛАР

1.1. Ахборот урушлар ва киберхужумлар

Хавфсизлик – ҳар куни биз тўқнашадиган ҳаётимизнинг жиҳати: эшикни қулфлаймиз, қимматбаҳо нарсаларни бегона кўзлардан беркитамиз ва ҳамённи дуч келган жойда қолдирмаймиз. Бу "рақамли дунёга" ҳам расм бўлиши шарт, чунки ҳар бир фойдаланувчининг компьютери қароқчи ҳужуми объекти бўлиши мумкин.

Коммерция ташкилотлари хавфсизликни таъминлаш ўзининг биринчи галдаги вазифаси эмас, балки уни таъминлашга сарф этиладиган ҳаражатларни муқаррар бало деб ҳисоблаб келганлар. Қандайдир даражада бу "оқилона иш": ниҳоят, усиз ҳам иш бажаришда тўсиқлар тўлиб-тошиб ётибдику?! Аммо фирманинг барча корпоратив биноларига кеча-кундуз киришга рухсат беришга журъат этувчи ақли жойида "саноат капитанлари"ни кўрганмисиз? Албатта, йўқ! Ҳатто кичкина компания биносининг кириш йўлида сизни қоровул, ёки киришни чегараловчи ва назоратловчи тизими қарши олади. Ахборотни ҳимоялаш эса ҳали кўнгилдагидек эмас. Ахборотни қандай йўқотиш мумкинлигини ва бу қандай оқибатларга олиб келишини барча ҳам тушунавермайди.

Йирик ўйинчилар яхшигина сабоқ олдилар: хакерлар Yahoo.com, Amazon.com каби компанияларга ва ҳатто космик тадқиқот агентилиги NASAга катта зарар етказдилар. Хавфсизлик хизмати бозорининг энг йирик номоёндаларидан бири RSA Security, ҳарқандай таҳдидга қарши чора борлиги хусусидаги ўйламасдан қилган баёнотидан бир неча кундан кейин, хужумга дучор бўлди[29].

Одатда одамлардан ёки предметлардан чиқадиган ва зарар етказадиган таҳдидлар қуйидаги синфларга бўлинади: *ички* ёки *ташқи* ва *тузилмаланган* (маълум объектга қарши) ёки *тузилмаланмаган* ("кимга Худо беради" қабилида адресланувчи). Масалан, компьютер вируслари "ташқи тузилмаланмаган таҳдидлар" сифатида туркумланади ва тамомила оддий ҳисобланади. Қизиғи шундаки, фойдаланувчилар ўзининг компьютерини

муайян нишон деб ҳисобламайдилар, улар ўзларини яхшигина ҳимоялангандек сезадилар. Керакли ҳимоя даражаси аксарият ҳолларда ишингизнинг ҳолатига боғлиқ. Агар ташкилотингиз ёки компаниянгиз қандайдир тазйиқ нишони бўлса, агар сиз миллий энергетик ресурсларни тақсимловчи ёки миллий алоқа тармоқларига хизмат қилувчи давлат инфратузилмаси таркибида бўлсангиз, оддий террористлар бомбаларини ва пистолетларини четга қўйиб, турли-туман дастурий воситалар ёрдамида ташкилотингизга электрон хужумни амалга ошириш масаласини кўрадилар. Иккинчи томондан, савдо-сотиқ ва маркетинг бўйича оддий ташкилот хусусида сўз борса, фақат мижозлар руйхатини ўғриловчи хизматчиларингиз тўғрисида, қалбаки кредит карточкалари бўйича товар олувчи фирибгарлар, тармоғингизга прейскурантлардан фойдаланиш мақсадида кирувчи рақиблар, Web-сайтингизни таъмагирлик мақсадида бузувчилар ва шунга ўхшашлар тўғрисида қайғуришингизга тўгри келади.

Аммо, ваҳимага ўрин йўқ. Биринчи навбатда кундалик эҳтиёж чоралари кўрилиши лозим. Ахборотга эга бўлишнинг энг оммабоп усули оддий ўғрилик. Сиз иш столингизда кечага мумайгина пулни қолдириб кетмайсизу. Нима учун боқувчингиз-шахсий компьютер хавфсизлигини таъминлашга озгина вақт сарф қилмайсиз? Бу нафақат аппарат воситаларига, балки маълумотларга ҳам тааллуқли. Маълумотларни ўғирлатиш ёки йўқотиш катта, баъзида, тузатиб бўлмайдиган зарар келтиради.

Маълумки, тизим маъмурлари барча маҳфий материаллардан фойдаланиш имконига эга ва, одатда, компания фойдасидан ўз улушларига эга эмаслар. Шу сабабли худди улар ташкилот хавфсизлигига таҳдид сола олувчилар ичида энг каттаси ҳисобланадилар. Таъкидлаш лозимки, компания ишга кирувчиларни синчиклаб текширади. Худди шундай, хавфсизлик хизматини таъминловчиларга, айниқса маслахат бериш, режалаштириш ва муъмурлашни тавсия этувчиларга диққат билан қараш лозим.

Цивилизация ривожининг замонавий босқичида ахборот нафақат жамоат ва давлат институтлари фаолиятида, балки ҳар бир инсон ҳаётида ҳал қилувчи ролни уйнайди. Кўз олдимизда жамиятнинг ахборотлашиши шиддат билан ва кўпинча олдиндан билиб бўлмайдиган тарзда ривожланмоқда.

Биз эса унинг ижтимоий, сиёсий, иқтисодий ва бошқа оқибатларини тушуниб етишга бошлаймиз, холос. Жамиятимизнинг ахборотлашиши ягона дунё ахборот маконининг яратилишига олиб келадики, бу макон доирасида ахборотни йиғиш, ишлаш, сақлаш ва субъектлар – инсонлар, ташкилотлар, давлатлар ўртасида алмашиш амалга оширилади.

Равшанки, сиёсий, иқтисодий, илмий-техникавий ва бошқа ахборотларни тезликда алмашиш имконияти жамият ҳаётининг барча соҳаларида ва айниқса ишлаб чиқаришда ва бошқаришда янги технологияларнинг қўлланилиши сўзсиз фойдалидир. Аммо, саноатнинг тезликда рифожланиши Ер экологиясига таҳдид сола бошлади, ядро физикаси соҳасидаги ютуқлар ядро уруши хавфини тўғдирди. Ахборотлаштириш ҳам жиддий муаммолар манбаига айланиши мумкин.

Урушлар доимо бўлган. Вақт ўтиши билан урушни олиб бориш бутун бир фанга айланди. Ҳарқандай фандагидек урушда ўзининг тарихи, ўзининг қоидаси, машҳур намоёндалари, ўзининг методологияси пайдо бўлди.

Замонавий уруш ғояси жуда илдамлаб кетди. Энди унинг макони – бутун ер шари. Уруш локал қароқчи хужумидан бир неча давлатларни вайрон қилувчи глобал муаммога айланди.

Турли мамлакатларнинг ҳарбий доктриналарида электрон қурол ривожи режалари ва махсус вазифаларга мўлжалланган дастурий таъминот тўғрисида эслатишлар кўзга ташланмоқда. Турли разведка манбаларидан келаётган ахборотнинг таҳлили натижасида хулоса қилиш мумкинки, баъзи бир давлатларнинг раҳбарлари хужумкор кибер-дастурларни яратишни молияламоқдалар.

Ахборот урушига оддий воситалар ёрдамида ҳарбий ҳаракатлар самара бермайдиган ҳолларга нисбатан стратегик альтернатива сифатида қаралмоқда.

Ҳарбийлар томонидан киритилган *ахборот уруши* атамаси реал, қирғинли ва емирувчи ҳарбий ҳаракатлар билан боғлиқ шафқатсиз ва хавфли фаолиятни англатади. Бу урушнинг алоҳида қирралари-штаб уруши, электрон уруши, психологик амаллар ва ҳ.

Ҳарқандай уруш, ахборот уруши шу жумладан, замонавий қурол ёрдамида олиб борилади. Ахборот қуроли ёрдамида, уруш олиб борилувчи барча қуроллардан фарқли ўлароқ, эълон қилинмаган ва кўпинча дунёга кўринмайдиган урушларни олиб бориш мумкин (олиб борилмоқда ҳам). Бу қуролнинг таъсир объектлари – иқтисодий, сиёсий, ижтимоий ва ҳ. каби жамият ва давлат институтлари. Маълумотларни узатиш тармоқларининг келажак жанглар майдонига айланиши аллақачон эътироф этилган.

Ахборот қуроли хужумда ва мудофаада "электрон тезлик" билан ишлатилиши мумкин. У энг илғор технологияларга асосланган бўлиб, ҳарбий низоларни дастлабки босқичида ҳал этилишини таъминлайди ҳамда умуммақсад кучларнинг қўлланилишини истисно қилади. Ахборот қуроли қўлланишининг стратегияси хужумкор характерга эга. Аммо хусусий заифлик нуқтаи назари мавжуд, айниқса фуқоролик секторида. Шу сабабли бундай қуролдан ва ахборот терроризмидан ҳимояланиш муаммоси ҳозирда биринчи ўринга чиққан. Фойдаланувчиларига дунё тармоқларида ишлашни таъминловчи мамлакатларнинг миллий ахборот ресурсларининг заифлиги – ҳар икки томонга хавфли нарса.

Ахборот қуроли деганда ахборот массивларини йўқотиш, бузиш ёки ўғирлаш воситалари, ҳимоялаш тизимини йўқотиш, қонуний фойдаланувчилар фаолиятини чегаралаш асбоб-ускуналар ва бутун компьютер тизими ишлаши тартибини бузиш воситалари тушунилади.

Ҳозирда хужумкор ахборот қуроли сифатида қуйидагиларни кўрсатиш мумкин:

- *компьютер вируслари* – кўпайиш, дастурларда ўрнашиш, алоқа линиялари, маълумотларни узатиш тармоқлари бўйича узатилиш, бошқариш тизимларни ишдан чиқариш ва шунга ўхшаш қобилиятларга эга;

- *мантиқий бомбалар* – сигнал бўйича ёки ўрнатилган вақтда ҳаракатга келтириш мақсадида ҳарбий ёки фуқаро инфратузилмаларига ўрнатилувчи дастурланган қурилмалар;

- *телекоммуникация тармоқларида ахборот алмашинувини бостириш воситалари*, давлат ва ҳарбий бошқарув каналларида ахборотни сохталаштириш;

- *тестли дастурларни бетарафлаштириш воситалари*;

- объект дастурий таъминотига айғоқчилар томонидан атайин киритилувчи турли хил *хатоликлар*.

Универсаллик, махфийлик, дастурий-аппарат амалга оширилишининг ҳар хиллиги, таъсирининг кескинлиги, қўлланилишининг вақти ва жойини танлаш имконияти, ниҳоят, фойдалилиги ахборот қуролини ҳаддан ташқари хавфли қилади. Бу қуролни, масалан, интеллектуал мулкни ҳимоялаш воситасига ўхшатиб ниқоблаш мумкин. Ундан ташқари, у ҳатто уруш эълон қилмасдан хужум ҳаракатларини автоном тарзда олиб бориш имконини беради.

Замонавий жамиятда ахборот қуролини ишлатиш ҳарбий стратегияси фуқаро сектори билан узвий боғланган. Ахборот қуролининг, унинг таъсири шакли ва усулларининг пайдо бўлиши ва қўлланиши хусусиятларининг турли-туманлилиги ундан ҳимояланишнинг мураккаб масалаларини вужудга келтирди.

Ахборот қуроли қўлланилишини олдини олиш ёки қўлланиши оқибатларини бартараф қилиш учун қуйидаги чораларни кўриш лозим:

- ахборот ресурсларининг физик асосини ташкил этувчи моддий-техник объектларни ҳимоялаш;

- маълумотлар базалари ва банкларининг меёрий ва муттасил ишлашини таъминлаш;

- ахборотдан рухсатсиз фойдаланишдан, уни бузилишидан ёки йўқ қилинишидан ҳимоялаш;

- ахборот сифатини сақлаш (ўз вақтидалиги, аниқлиги, тўлалиги ва фойдаланувчанлиги).

Давлатнинг дунё очиқ тармоғига уланишининг иқтисодий ва илмий-техник сиёсатини ахборот хавфсизлиги орқали кўриш лозим. Бу очиқ, фуқароларнинг ахборотга ва интеллектуал мулкга эга бўлиш қонуний ҳуқукини сақлашга мўлжалланган сиёсат мамлакат худудида тармоқ асбоб-ускуналарини унга ахборот қуроли элементларининг киришидан сақлашни кўзда тутиш лозим. Бу муаммо ҳозирда, чет эл ахборот технологияларини оммавий сотиб олинаётган пайтда ўта муҳимдир.

Маълумки, дунё ахборот маконига уланмасдан мамлакат иқтисодини ривожлантириб бўлмайди. Internet тармоғи томонидан таъминланган ахборот ва ҳисоблаш ресурсларидан оператив фойдаланишни давлатчиликни, фуқаролик жамияти институтларини мустаҳкамлаш, ижтимоий инфратузилмаларининг ривожланиш шартлари сифатида талқин этиш мумкин.

Аммо мамлакатнинг ҳалқаро телекоммуникация тизимида ва ахборот алмашинувида иштирокининг ахборот хавфсизлиги муаммосини комплекс ҳал қилмасдан мумкин эмаслигини аниқ тасаввур этиш лозим. Айниқса хусусий ахборот ресурсларини ҳимоялаш муаммоси ахборот ва телекоммуникация технологиялар соҳасида ривожланган мамлакатлардан технологик орқада қолаётган мамлакатлар учун жиддий ҳисобланади.

Ахборот қуролини ишлаб чиқишни ва уни ишлатишни химиявий ва бактериологик қурол каби тақиқлаш эҳтимолдан узоқ. Худди шу каби кўпгина мамлакатларнинг ягона глобал ахборот маконини шакллантириш бўйича уринишларини чегаралаб бўлмайди.

Тизим маъмури учун ҳимоянинг мақбул даражасини таъминлашнинг ягона усули-ахборотга эга бўлиши, чунки ҳозирча ахборот хужумига энг тез реакция берадиган инсон ҳисобланади. Демак, ахборотни ҳимоялаш маъмурларининг ўқитишга ва профессионал ўсишига сарф-ҳаражат ахборот хужумларига қарши турувчи энг самарали восита ҳисобланади.

1.2. Ахборот-коммуникацион тизимлар ва тармоқларда таҳдидлар ва заифликлар

Тармоқ технологиялари ривожининг бошланғич босқичида вируслар ва компьютер хужумларининг бошқа турлари таъсиридаги зарар кам эди, чунки у даврда дунё иқтисодининг ахборот технологияларига боғлиқлиги катта эмас эди. Ҳозирда, хужумлар сонининг доимо ўсиши ҳамда бизнеснинг ахборотдан фойдаланиш ва алмашишнинг электрон воситаларига боғлиқлиги шароитида машина вақтининг йўқолишига олиб келувчи ҳатто озгина хужумдан келган зарар жуда катта рақамлар орқали ҳисобланади. Мисол тариқасида келтириш мумкинки, фақат 2003 йилнинг биринчи чора-

гида дунё миқёсидаги йўқотишлар 2002 йилдаги барча йўқотишлар йиғиндисининг 50%ини ташкил этган, ёки бўлмаса 2006 йилнинг ўзида Россия Федереациясида 14 мингдан ортиқ компьютер жиноятчилиги ҳолатлари қайд этилган[29, 30, 32].

Корпоратив тармоқларда ишланадиган ахборот, айниқса, заиф бўлади. Ҳозирда рухсатсиз фойдаланишга ёки ахборотни модификациялашга, ёлғон ахборотнинг муомалага кириши имконининг жиддий ошишига қуйидагилар сабаб бўлади:

- компьютерда ишланадиган, узатиладиган ва сақланадиган ахборот ҳажмининг ошиши;

- маълумотлар базасида муҳимлик ва маҳфийлик даражаси турли бўлган ахборотларнинг тўпланиши;

- маълумотлар базасида сақланаётган ахборотдан ва ҳисоблаш тармоқ ресурларидан фойдаланувчилар доирасининг кенгайиши;

- масофадаги ишчи жойлар сониниг ошиши;

- фойдаланувчиларни боғлаш учун Internet глобал тармоғини ва алоқанинг турли каналларини кенг ишлатиш;

- фойдалувчилар компьютерлари ўртасида ахборот алмашинувининг автоматлаштирилиши.

Ахборот хавфсизлигига таҳдид деганда ахборотнинг бузилиши ёки йўқотилиши хавфига олиб келувчи ҳимояланувчи объектга қарши қилинган ҳаракатлар тушунилади. Олдиндан шуни айтиш мумкинки, сўз барча ахборот хусусида эмас, балки унинг фақат, мулк эгаси фикрича, коммерция қийматига эга бўлган қисми хусусида кетяпти.

Замонавий корпоратив тармоқлар ва тизимлар дучор бўладиган кенг тарқалган таҳдидларни таҳлиллаймиз. Ҳисобга олиш лозимки, хавфсизликка таҳдид манбалари корпоратив ахборот тизимининг ичида (ички манба) ва унинг ташқарисида (ташқи манба) бўлиши мумкин. Бундай ажратиш тўғри, чунки битта таҳдид учун (масалан, ўғирлаш) ташқи ва ички манбаларга қарши ҳаракат усуллари турлича бўлади. Бўлиши мумкин бўлган таҳдидларни ҳамда корпоратив ахборот тизимининг заиф жойларини билиш

хавфсизликни таъминловчи энг самарали воситаларни танлаш учун зарур ҳисобланади.

Тез-тез бўладиган ва хавфли (зарар ўлчами нуқтаи назаридан) таҳдидларга фойдаланувчиларнинг, операторларнинг, маъмурларнинг ва корпоратив ахборот тизимларига хизмат кўрсатувчи бошқа шахсларнинг атайин қилмаган хатоликлари киради. Баъзида бундай хатоликлар (нотўғри киритилган маълумотлар, дастурдаги хатоликлар сабаб бўлган тизимнинг тўхташи ёки бўзилиши) тўғридан тўғри зарарга олиб келади. Баъзида улар нияти бузуқ одамлар фойдаланиши мумкин бўлган нозик жойларни пайдо бўлишига сабаб бўлади. Глобал ахборот тармоғида ишлаш ушбу омилнинг етарлича долзарб қилади. Бунда зарар манбаи ташкилотнинг фойдаланувчиси ҳам, тармоқ фойдаланувчиси ҳам бўлиши мумкин, охиргиси айниқса хавфли.

Зарар ўлчами бўйича иккинчи ўринни ўғирлашлар ва сохталаштиришлар эгаллайди. Текширилган ҳолатларнинг аксариятида ишлаш режимлари ва ҳимоялаш чоралари билан аъло даражада таниш бўлган ташкилот штатидаги ходимлар айбдор бўлиб чиқдилар. Глобал тармоқлар билан боғланган қувватли ахборот каналининг мавжудлигида, унинг ишлаши устидан етарлича назорат йўқлиги бундай фаолиятга қўшимча имкон яратади.

Хафа бўлган ходимлар (ҳатто собиқлари) ташкилотдаги тартиб билан таниш ва жуда самара билан зиён етказишлари мумкин. Ходим ишдан бўшаганида унинг ахборот ресурсларидан фойдаланиш хуқуқи бекор қилиниши назоратга олиниши шарт.

Ҳозирда ташқи коммуникация орқали рухсатсиз фойдаланишга атайин қилинган уринишлар бўлиши мумкин бўлган барча бузилишларнинг 10%ини ташкил этади. Бу катталик анчагина бўлиб туюлмаса ҳам, Internetда ишлаш тажрибаси кўрсатадики, қарийб ҳар бир Internet-сервер кунига бир неча марта суқилиб кириш уринишларига дучор бўлар экан. Хавф-хатарлар тахлил қилинганида ташкилот корпоратив ёки локал тармоғи компьютерларининг хужумларга қарши туриши ёки бўлмаганида ахборот хавфсизлиги бузилиши фактларини қайд этиш учун етарлича ҳимояланмаганлигини ҳисобга олиш зарур. Масалан, ахборот тизимларини

ҳимоялаш Агентлигининг (АҚШ) тестлари кўрсатадики, 88% компьютерлар ахборот хавфсизлиги нуқтаи назаридан нозик жойларга эгаки, улар рухсатсиз фойдаланиш учун фаол ишлатишлари мумкин. Ташкилот ахборот тузилмасидан сасофадан фойдаланиш холлари алоҳида кўрилиши лозим.

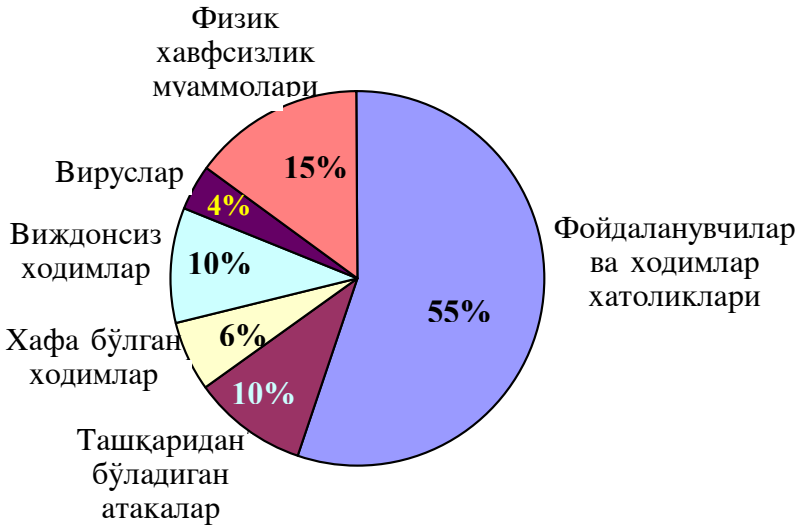
Ҳимоя сиёсатини тузишдан аввал ташкилотда компьютер муҳити дучор бўладиган хавф-хатар баҳоланиши ва зарур чоралар кўрилиши зарур. Равшанки, ҳимояга таҳдидни назоратлаш ва зарур чораларни кўриш учун ташкилотнинг сарф-ҳаражати ташкилотда активлар ва ресурсларни ҳимоялаш бўйича ҳеч қандай чоралар кўрилмаганида кутиладиган йўқотишлардан ошиб кетмаслиги шарт.

Умуман олганда, ташкилотнинг компьютер муҳити икки хил хавф-хатарга дучор бўлади:

1. Маълумотларни йўқотилиши ёки ўзгартирилиши.
2. Сервиснинг тўхтатилиши.

Таҳдидларнинг манбаларини аниқлаш осон эмас. Улар нияти бузуқ одамларнинг бостириб киришидан то компьютер вирусларигача турланиши мумкин.

Бунда инсон хатоликлари хавфсизликка жиддий таҳдид ҳисобланади. 1.1-расмда корпоратив ахборот тизимида хавфсизликнинг бузилиш манбалари бўйича статистик маълумотларни тасвирловчи айланма диаграмма келтирилган.



1.1-расм. Хавфсизликнинг бузилиш манбалари.

1.1.-расмда келтирилган статистик маълумотлар ташкилот маъмуриятига ва ходимларига корпоратив тармоқ ва тизими хавфсизлигига таҳдидларни самарали камайтириш учун харакатларни қаерга йўналтиришлари зарурлигини айтиб бериши мумкин. Албатта, физик хавфсизлик муаммолари билан шуғулланиш ва инсон хатоликларининг хавфсизликка салбий таъсирини камайтириш бўйича чоралар кўрилиши зарур. Шу билан бир қаторда корпоратив тармоқ ва тизимга ҳам ташқаридан, ҳам ичкаридан бўладиган хужумларни олдини олиш бўйича тармоқ хавфсизлиги масаласини ечишга жиддий эътиборни қаратиш зарур.

1.3. Компьютер жиноятчилигининг таҳлили

Компьютер жиноятчилиги статистикаси таҳлил этилса қайғули манзарага эга бўламиз. Компьютер жиноятчилиги етказган зарарни наркотик моддалар ва қуролларнинг ноқонуний айланишидан олинган фойдага қиёслаш мумкин. Фақат АҚШда "электрон жиноятчилар" етказган ҳар йилги зарар қарийб 100 млд. долларни ташкил этар экан.

Яқин келажакда жиноий фаолиятнинг бу тури даромадлилиги, пул маблағларининг айланиши ва унда иштирок этувчи одамлар сони бўйича яқин вақтларгача ноқонуний фаолият орасида даромадлиги билан биринчи ўринни эгаллаган ноқонуний бизнеснинг уч туридан узиб кетиш эҳтимоллиги катта. Бу ноқонуний бизнеслар-наркотик моддалар, қурол ва кам учрайдиган ёввойи ҳайвонлар билан савдо қилиш.

Давлат ва хусусий компаниялар фаолиятининг социологик тадқиқи маълумотларига қараганда XXI асрнинг биринчи йилларида иқтисодий соҳадаги жиноятчилик банк ва бошқа тизимларнинг ахборот-коммуникацион комплексларига бўлиши мумкин бўлган ғаразли иқтисодий ҳаракатларга қаратилган бўлади.

Кредит-молия соҳасидаги компьютер жиноятчилигининг сони муттасил ўсиб бормоқда. Масалан онлайн магазинларида 25%гача қаллоблик тўлов амаллари қайд этилган. Шунга қарамасдан Ғарб давлатларида электрон тижоратнинг-юқори даромадли замонавий бизнеснинг фаол ривожланиши кўзга ташланмоқда. Маълумки, бу соҳа ривожланиши билан параллел

равишда "виртуал" қаллобларнинг ҳам даромади ошади. Қаллоблар энди якка ҳолда ҳаракат қилмайдилар, улар пухталик билан тайёрланган, яхши техник ва дастурий қуролланган жиноий гуруҳлар билан, банк хизматчиларининг ўзлари иштирокида ишлайдилар.

Хавфсизлик соҳасидаги мутахассисларнинг кўрсатишича бундай жиноятчиларнинг улуши 70%ни ташкил этади. "Виртуал" ўғри ўзининг ҳамкасби-оддий босқинчига нисбатан кўп топади. Ундан ташқари "виртуал" жиноятчилар уйидан чиқмасдан ҳаракат қиладилар. Фойдаланишнинг электрон воситаларини ишлатиб қилинган ўғрилик зарарининг ўртача кўрсаткичи фақат АҚШда банкни қуролли босқинчиликдан келган зарарнинг ўртача статистик зараридан 6-7 марта катта.

Банк хизмати ва молия амаллари соҳасидаги турли хил қаллоблик натижасида йўқотишлар 1989 йили 800 млн. доллардан 1997 йили – 100 млрд. долларга етган. Бу кўрсаткичлар ўсаяпти, аслида юқорида келтирилган маълумотлардан бир тартибга ошиши мумкин. Чунки кўп йўқотишлар аниқланмайди ёки эълон қилинмайди. Ўзига хос "*индамаслик сиёсати*"ни тизим маъмурларининг ўзининг тармоғидан рухсатсиз фойдаланганлик тафсилотини, бу нохуш ходисанинг такрорланишидан қўрқиб ва ўзининг ҳимоя усулини ошкор этмаслик важида муҳокама этишни хохламасликлари билан тушуниш мумкин.

Компьютер ишлатиладиган инсон фаолиятининг бошқа соҳаларида ҳам вазият яхши эмас. Йилдан-йилга хуқуқни муҳофаза қилувчи органларига компьютер жиноятчилиги хусусидаги мурожаатлар ошиб бормоқда.

Барча мутахассислар вирусларнинг тарқалиши билан бир қаторда ташқи хужумларнинг кескин ошганлигини эътироф этмоқдалар. Кўриниб турибдики, компьютер жиноятчилиги натижасида зарар қатъий ортмоқда. Аммо компьютер жиноятчилиги кўпинча "виртуал" қаллоблар томонидан амалга оширилади дейиш ҳақиқатга тўғри келмайди. Ҳозирча компьютер тармоқларига суқилиб кириш хавфи ҳар бири ўзининг усулига эга бўлган хакерлар, кракерлар ва компьютер қароқчилари томонидан келмоқда.

Хакерлар, бошқа компьютер қароқчиларидан фарқли ҳолда, баъзида, олдиндан, мақтаниш мақсадида компьютер эгаларига уларнинг тизимига ки-

риш ниятлари борлигини билдириб қўядилар. Муваффақиятлари хусусида Internet сайтларида хабар берадилар. Бунда хакер мусобақалашув ниятида кирган компьютерларига зарар етказмайди.

Кракерлар (cracker) – электрон "ўғрилар" манфаат мақсадида дастурларни бузишга ихтисослашганлар. Бунинг учун улар Internet тармоғи бўйича тарқатилувчи бузишнинг тайёр дастурларидан фойдаланадилар.

Компьютер қароқчилари – рақобат қилувчи фирмалар ва хатто ажнабий махсус хизматлари буюртмаси бўйича ахборотни ўғирловчи фирма ва компанияларнинг юқори малакали мутахассислари. Ундан ташқари улар бегона банк счетидан пул маблағларини ўғирлаш билан ҳам шуғулланадилар.

Баъзи "мутахассислар" жиддий гуруҳ ташкил қиладилар, чунки бундай криминал бизнес ўта даромадлидир. Бу эса тез орада, "виртуал" жиноятнинг зарари жиноят бизнесининг анъанавий хилидаги зарардан бир тартибга (агар кўп бўлмаса) ошишига сабаб бўлади. Ҳозирча бундай таҳдидни бетарафлаштиришнинг самарали усуллари мавжуд эмас.

1.4. Тармоқдаги ахборотга бўладиган намунавий хужумлар

Барча хужумлар Internet ишлаши принципларининг қандайдир чегараланган сонига асосланганлиги сабабли масофадан бўладиган намунавий хужумларни ажратиш ва уларга қарши қандайдир комплекс чораларни тавсия этиш мумкин. Бу чоралар, ҳақиқатан, тармоқ хавфсизлигини таъминлайди.

Internet протоколларининг мукаммал эмаслиги сабабали тармоқдаги ахборотга масофадан бўладиган асосий намунавий хужумлар қуйидагилар:

- тармоқ трафигини тахлиллаш;
- тармоқнинг ёлғон обьектини киритиш;
- ёлғон маршрутни киритиш;
- хизмат қилишдан воз кечишга ундайдиган хужумлар.

Тармоқ трафигини тахлиллаш. Сервердан Internet тармоғи базавий протоколлари FTP (File Transfer Protocol) ва TELNET (Виртуал терминал протоколи) бўйича фойдаланиш учун фойдаланувчи *идентификация* ва *аутентификация* муолажаларини ўтиши лозим. Фойдаланувчини идентифика-

циялашда ахборот сифатида унинг идентификатори (исми) ишлатилса, аутентификациялаш учун *парол* ишлатилади. FTP ва TELNET протоколларининг хусусияти шундаки, фойдалувчиларнинг пароли ва идентификатори тармоқ орқали очиқ, шифрланмаган кўринишда узатилади. Демак, Internet хостларидан фойдаланиш учун фойдаланувчининг исми ва паролини билиш кифоя.

Ахборот алмашинувида Internetнинг масофадаги иккита узели алмашинув ахборотини *пакетларга* бўлишади. Пакетлар алоқа каналлари орқали узатилади ва шу пайтда ушлаб қолиниши мумкин.

FTP ва TELNET протоколларининг тахлили кўрсатадики, TELNET паролни символларга ажратади ва паролнинг ҳар бир символини мос пакетга жойлаштириб битталаб узатади, FTP эса, аксинча, паролни бутунлайича битта пакетда узатади. Пароллар шифрланмаганлиги сабабли пакетларнинг махсус сканер-дастурлари ёрдамида фойдаланувчининг исми ва пароли бўлган пакетни ажратиб олиш мумкин. Худди шу сабабли, ҳозирда оммавий тус олган ICQ дастури ҳам ишончли эмас. ICQнинг протоколлари ва ахборотларни сақлаш, узатиш форматлари маълум ва демак, унинг трафиги ушлаб қолиниши ва очилиши мумкин.

Асосий муаммо алмашинув протоколида. Базавий татбиқий проколларнинг TCP/IP оиласи анча олдин (60 йилларнинг охири ва 80-йилларнинг боши) ишлаб чиқилган ва ундан бери умуман ўзгартирилмаган. Ўтган давр мобайнида тақсимланган тармоқ хавфсизлигини таъминлашга ёндашиш жиддий ўзгарди. Тармоқ уланишларини ҳимоялашга ва трафикни шифрлашга имкон берувчи ахборот алмашинувининг турли протоколлари ишлаб чиқилди. Аммо бу протоколлар эскиларининг ўрнини олмади (SSL бундан истисно) ва стандарт мақомига эга бўлмади. Бу протоколларининг стандарт бўлиши учун эса тармоқдан фойдаланувчиларнинг барчаси уларга ўтишлари лозим. Аммо, Internetда тармоқни марказлашган бошқариш бўлмаганлиги сабабли бу жараён яна кўп йиллар давом этиши мумкин.

Тармоқнинг ёлғон объектини киритиш. Ҳар қандай тақсимланган тармоқда қидириш ва адреслаш каби "нозик жойлари" мавжуд. Ушбу жараёнлар кечишида тармоқнинг ёлғон объектини (одатда бу ёлғон хост) кири-

тиш имконияти туғилади. Ёлғон обьектнинг киритилиши натижасида адресатга узатмоқчи бўлган барча ахборот аслида нияти бузуқ одамга тегади. Тахминан буни тизимингизга, одатда электрон почтани жўнатишда фойдаланадиган провайдерингиз сервери адреси ёрдамида киришга кимдир уддасидан чиққани каби тасаввур этиш мумкин. Бу ҳолда нияти бузуқ одам унчалик қийналмасдан электрон хат-хабарингизни эгаллаши, мумкин, сиз эса хатто ундан шубхаланмасдан ўзингиз барча электрон почтангизни жўнатган бўлар эдингиз.

Қандайдир хостга мурожаат этилганида адресларни махсус ўзгартиришлар амалга оширилади (IP-адресдан тармоқ адаптери ёки маршрутизаторининг физик адреси аниқланади). Internetда бу муаммони ечишда ARP(Adress Resolution Protocol) протоколидан фойдаланилади. Бу қуйидагича амалга оширилади: тармоқ ресурсларига биринчи мурожаат этилганида хост кенг кўламли ARP-сўровни жўнатади. Бу сўровни тармоқнинг берилган сегментидаги барча станциялар қабул қилади. Сўровни қабул қилиб, хост сўров юборган хост хусусидаги ахборотни ўзининг ARP-жадвалига киритади, сўнгра унга ўзининг Ethernet-адреси бўлган ARP-жавобни жўнатади. Агар бу сегментда бундай хост бўлмаса, тармоқнинг бошқа сегментларига мурожаатга имкон берувчи маршрутизаторга мурожаат қилинади. Агар фойдаланувчи ва нияти бузуқ одам бир сегментда бўлса, ARP-сўровни ушлаб қолиш ва ёлғон ARP-жавобни йўллаш мумкин бўлади. Бу усулнинг таъсири фақат битта сегмент билан чегараланганлиги тасалли сифатида хизмат қилиши мумкин.

ARP билан бўлган холга ўхшаб DNS-суровни ушлаб қолиш йўли билан Internet тармоғига ёлғон DNS-серверни киритиш мумкин.

Бу қуйидаги алгоритм бўйича амалга оширилади:

1. DNS-сўровни кутиш.
2. Олинган сўровдан керакли маълумотни чиқариб олиш ва тармоқ бўйича сўров юборган хостга ёлғон DNS-жавобни ҳақиқий DNS-сервер номидан узатиш. Бу жавобда ёлғон DNS-сервернинг IP-адреси кўрсатилган бўлади.

3. Хостдан пакет олинганида пакетнинг IP-сарлавхасидаги IP-адресни ёлғон DNS сервернинг IP-адресига ўзгартириш ва пакетни серверга узатиш (яъни ёлғон DNS-сервер ўзининг номидан сервер билан иш олиб боради).
4. Сервердан пакетни олишда пакетнинг IP-сарлавҳасидаги IP-адресни ёлғон DNS-сервернинг IP-адресига ўзгартириш ва пакетни хостга узатиш (ёлғон DNS серверни хост ҳақиқий ҳисоблайди).

Ёлғон маршрутни киритиш. Маълумки, замонавий глобал тармоқлари бир-бири билан *тармоқ узеллари* ёрдамида уланган тармоқ сегментларининг мажмуидир. Бунда *маршрут* деганда маълумотларни манбадан қабул қилувчига узатишга хизмат қилувчи тармоқ узелларининг кетма-кетлиги тушунилади. Маршрутлар хусусидаги ахборотни алмашишни унификациялаш учун маршрутларни бошқарувчи махсус протоколлар мавжуд. Internetдаги бундай протоколларга янги маршрутлар хусусида хабарлар алмашиш протоколи – ICMP (Internet Control Message Protocol) ва маршрутизаторларни масофадан бошқариш протоколи SNMP (Simple Network Manegment Protocol) мисол бўлаолади. Маршрутни ўзгартириш хужум қилувчи ёлғон хостни киритишдан бўлак нарса эмас. Хатто охирги обьект ҳақиқий бўлса, ҳам маршрутни ахборот барибир ёлғон хостдан ўтадиган қилиб қуриш мумкин.

Маршрутни ўзгартириш учун хужум қилувчи тармоққа тармоқни бошқарувчи қурилмалар (масалан, маршрутизаторлар) номидан берилган тармоқни бошқарувчи протоколлар орқали аниқланган махсус хизматчи хабарларни жўнатиши лозим. Маршрутни муваффақиятли ўзгартириш натижасида хужум қилувчи тақсимланган тармоқдаги иккита обьект алмашадиган ахборот оқимидан тўла назоратга эга бўлади, сўнгра ахборотни ушлаб қолиши, тахлиллаши, модификациялаши ёки оддийгина йўқотиши мумкин. Бошқача айтганда таҳдидларнинг барча турларини амалга ошириш имконияти туғилади.

Хизмат қилишдан воз кечишга ундайдиган тақсимланган хужумлар – DdoS (Distributed Denial of Service) компьютер жиноятчилигининг нисбатан янги хили бўлсада, қўрқинчли тезлик билан тарқалмоқда. Бу хужум-

ларнинг ўзи анчагина ёқимсиз бўлгани етмаганидек, улар бир вақтнинг ўзида масофадан бошқарилувчи юзлаб хужум қилувчи серверлар томонидан бошланиши мумкин.

Хакерлар томонидан ташкил этилган узелларда DDoS хужумлар учун учта инструментал воситани топиш мумкин: trinoo, Tribe FloodNet (TFN) ва TFN2K. Яқинда TFN ва trinoonинг энг ёқимсиз сифатларини уйғунлаштирган яна биттаси stacheldraht ("тикон симлар") пайдо бўлди.

1.2-расмда хизмат қилишдан воз кечишга ундайдиган хужум воситаларининг характеристикалари келтирилган.

Хизмат қилишдан воз кечишга ундайдиган оддий тармоқ хужумида хакер танлаган тизимига пакетларни жунатувчи инструментидан фойдаланади. Бу пакетлар нишон тизимининг тўлиб тошиши ва бузилишига сабаб бўлиши керак. Кўпинча бундай пакетларни жунатувчилар адреси бузиб кўрсатилади. Шу сабабли хужумнинг ҳақиқий манбасини аниқлаш жуда қийин.

1.2-расм. Хизмат килишдан воз кечишга ундайдиган хужум воситаларининг характеристикалари

DDoS хужумларини ташкил этиш битта хакернинг қўлидан келади, аммо бундай хужумнинг эффекти *агентлар* деб аталувчи хужум қилувчи

серверларнинг ишлатилиши ҳисобига анчагина кучаяди. TFNда *серверлар* (server), а trinoода *демонлар* (daemon) деб аталувчи бу агентлар хакер томонидан масофадан бошқарилади.

1.5. Ахборот хавфсизлигини бузувчининг модели

Бўлиши мумкин бўлган таҳдидларни олдини олиш учун нафақат операцион тизимларни, дастурий таъминотни ҳимоялаш ва фойдаланишни назорат қилиш, балки бузувчилар туркумини ва улар фойдаланадиган усулларни аниқлаш лозим.

Сабаблар, мақсадлар ва усулларга боғлиқ ҳолда ахборот хавфсизлигини бузувчиларни тўртта категорияга ажратиш мумкин:

- саргузашт қидирувчилар;
- ғоявий хакерлар;
- хакерлар-профессионаллар;
- ишончсиз ходимлар.

Саргузашт қидирувчи, одатда, ёш, кўпинча талаба ёки юқори синф ўқувчиси ва унда ўйлаб қилинган хужум режаси камдан-кам бўлади. У нишонини тасодифан танлайди, қийинчиликларга дуч келса чекинади. Хавфсизлик тизимида нуқсонли жойни топиб, у махфий ахборотни йиғишга тиришади, аммо ҳеч қачон уни яширинча ўзгартиришга уринмайди. Бундай саргузашт қидирувчи муваффақиятларини факат яқин дўстлари–касбдошлари билан ўртоқлашади.

Ғояли хакер – бу ҳам саргузашт қидурувчи, аммо моҳирроқ. У ўзининг эътиқоди асосида муайян нишонларни (хостлар ва ресурсларни) танлайди. Унинг яхши кўрган хужум тури Web-сервернинг ахборотини ўзгартириши ёки, жуда кам ҳолларда, хужум қилинувчи ресурслар ишини блокировка қилиш. Саргузашт қидирувчиларга нисбатан ғояли хакерлар муваффақиятларини кенгрок аудиторияда, одатда ахборотни хакер Web-узелда ёки Usenet анжуманида жойлаштирилган ҳолда эълон қиладилар.

Хакер-проффесионал ҳаракатларнинг аниқ режасига эга ва маълум ресурсларни мўлжаллайди. Унинг хужумлари яхши ўйланган ва одатда бир

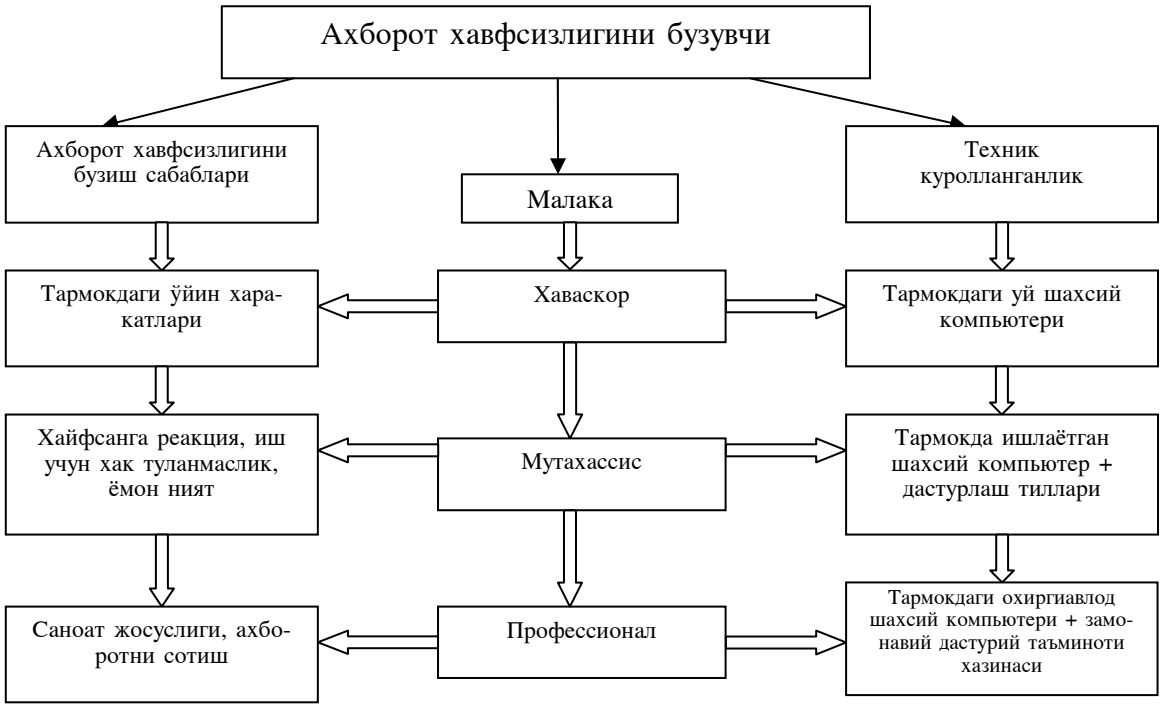
неча босқичда амалга оширилади. Аввал у дастлабки ахборотни йиғади (операцион тизим тури, тақдим этиладиган сервислар ва қўлланиладиган ҳимоя чоралари). Сўнгра у йиғилган маълумотларни ҳисобга олган ҳолда хужум режасини тузади ва мос инструментларни танлайди (ёки ҳатто ишлаб чиқади). Кейин, хужумни амалга ошириб, махфий ахборотни олади ва ниҳоят ҳаракатларининг барча изларини йўқ қилади. Бундай хужум қилувчи профессионал, одатда яхши молияланади ва якка ёки профессионаллар командасида ишлаши мумкин.

Ишончсиз ходим ўзининг ҳаракатлари билан саноат жосуси етказадиган муаммога тенг (ундан ҳам кўп бўлиши мумкин) муаммони тўғдиради. Бунинг устига унинг борлигини аниқлаш мураккаброқ. Ундан ташқари унга тармоқнинг ташқи ҳимоясини эмас, балки фақат, одатда унчалик катьий бўлмаган тармоқнинг ички ҳимоясини бартараф қилишига тўғри келади. Аммо, бу ҳолда унинг корпоратив маълумотлардан рухсатсиз фойдаланиши хавфи бошқа ҳар қандай нияти бузуқ одамникидан юқори бўлади.

Юқорида келтирилган ахборот хавфсизлигини бузувчилар категорияларини уларни малакалари бўйича гуруҳлаш мумкин: хаваскор (саргузашт қидирувчи), мутахассис (ғояли хакер, ишончсиз ходим), профессионал (хакер-профессионал). Агар бу гуруҳлар билан хавфсизликнинг бузилиши сабаблари ва ҳар бир гуруҳнинг техник қуролланганлиги таққосланса, ахборот хавфсизлигини бузувчининг умумлаштирилган моделини олиш мумкин (1.3-расм).

Ахборот хавфсизлигини бузувчи, одатда маълум малакали мутахассис бўлган ҳолда компьютер тизимлари ва тармоқлари хусусан, уларни ҳимоялаш воситалари хусусида барча нарсаларни билишга уринади. Шу сабабли бузувчи модели қуйидагиларни аниклайди:

- бузувчи бўлиши мумкин бўлган шахслар категорияси;
- бузувчининг бўлиши мумкин бўлган нишонлари ва уларнинг муҳимлик ва хавфсизлик даражаси бўйича рутбаланиши;
- унинг малакаси хусусидаги тахминлар; унинг техник қуролланганлигининг бахоси;
- унинг ҳаракат ҳарактери бўйича чеклашлар ва тахминлар.



1.3-расм. Ахборот хавфсизлигини бузувчининг модели

Тизимдан рухсатсиз фойдаланишга мажбур этиш сабабларининг диапазони етарлича кенг: компьютер билан ўйнаганидаги хаяжон кўтаринкилигидан то жирканч менеджер устидан хокимлик хиссиётигача. Бу билан нафақат кўнгил очишни хохловчи хаваскорлар, балки профессионал дастурчилар ҳам шуғулланади. Улар паролни танлаш, фараз қилиш натижасида ёки бошқа хакерлар билан алмашиш йўли орқали қулга киритадилар. Уларнинг бир қисми нафақат файлларни кўриб чиқади, балки файлларнинг мазмуни билан қизиқа бошлайди. Бу жиддий таҳдид ҳисобланади, чунки бу ҳолда беозор шухликни ёмон ният билан қилинган ҳаракатдан ажратиш қийин бўлади.

Яқин вақтгача раҳбарлардан норози хизматчиларнинг ўз мавқеларини суиистеъмол қилган ҳолда тизимни бузишлари, ундан бегоналарнинг фойдаланишларига йўл қўйишлари ёки тизимни иш ҳолатида қаровсиз қолдиришлари ташвишлантирар эди. Бундай ҳаракатларга мажбур этиш сабаблари қуйидагилар:

- хайфсанга ёки раҳбар томонидан танбеҳга реакция;

- иш вақтидан ташқари бажарилган ишга фирма ҳақ тўламаганидан норозилик;

- фирмани қандайдир янги тузилаётган фирмага рақиб сифатида заифлаштириш мақсадида қасос олиш каби ёмон ният.

Рахбардан норози ходим жамоа фойдаланувчи ҳисоблаш тизимларига энг катта таҳдидлардан бирини туғдиради. Шунинг учун ҳам хакерлар билан курашиш агентлиги индивидуал компьютер соҳибларига жон деб хизмат кўрсатадилар.

Профессионал хакерлар-ҳисоблаш техникасини ва алока тизимини жуда яхши биладиган компьютер фанатлари (мутаассиблари) ҳисобланади. Тизимга кириш учун профессионаллар омадга ва фаразга таянмайдилар ва қандайдир тартибни ва тажрибани ишлатадилар. Уларнинг максади-ҳимояни аниқлаш ва йўқотиш, ҳисоблаш курилмасининг имкониятларини ўрганиш ва мақсадига эришиш мумкинлиги тўғрисида қарорга келиш.

Бундай профессионал хакерлар категориясига қуйидаги шахслар киради:

- сиёсий мақсадни кўзловчи жиноий гуруҳларга кирувчилар;
- саноат жосуслик мақсадларида ахборотни олишга уринувчилар;
- текин даромадга интилувчи хакерлар гуруҳи.

Умуман профессионал хакерлар хавф-хатарни минималлаштиришга уринадилар. Бунинг учун улар бирга ишлашга фирмада ишлайдиган ёки фирмадан яқинда ишдан бўшатилган ходимларни жалб этадилар, чунки бегона учун банк тизимига киришда ошкор бўлиш хавфи жуда катта. Хақиқатан, банк ҳисоблаш тизимларининг мураккаблиги ва юқори тезкорлиги, хужжатларни юргизиш ва текшириш усулларининг мунтазам такомиллаштирилиши бегона шахс учун хабарларни ушлаб колиш ёки маълумотларни ўғирлаш мақсадида тизимга ўрнашишига имкон бермайди. Профессионал хакерлар учун яна бир қўшимча хавотир-тизимдаги бир компонентнинг ўзгариши бошқа бир компонентнинг бузилишига олиб келиши ва хатардан дарак берувчи сигналга сабаб бўлиши мумкин.

Хакерлар хавф-хатарни камайтириш мақсадида одатда молиявий ва оилавий муаммоларга эга бўлган ходимлар билан контактга кирадилар. Кўпгина одамлар ҳаётида хакерлар билан тўқнашмасликлари мумкин, аммо алкаголга ёки қиморга ружу қўйган ходимлар билмасдан жиноий гуруҳ би-

лан боғланган қандайдир бир букмекердан қарздор бўлиб қолишлари мумкин. Бундай ходим қандайдир ўйин-кулги кечасида суҳбатдошининг профессионал агент эканлигига шубҳа қилмаган ҳолда ортиқча гапириб юбориши мумкин.

II боб. ЭЛЕКТРОН БИЗНЕС ВА УНИНГ ХАВФСИЗЛИГИ МУАММОЛАРИ

2.1 Internet нинг асосий ахборот хизматлари

Internet тармоғи коммуникациянинг ва ахборотдан фойдаланишнинг турли-туман усулларини таклиф этади. Шу сабабли у тезликда кўпгина компаниялар ахборот тизимларининг ажралмас қисми бўлиб қолди. Internet тармоғи ҳар қандай абонентлар учун маълумотларни транзит узатиш бўйича транспорт хизматларидан ташқари юқори савияли тармоқ сервисларининг (хизматларининг) етарли даражада кенг тўпламини ҳам таъминлайди. Бу хизматларни тақдим этувчи компьютерлар серверлар деб аталса бу хизматлардан фойдаланувчи компьютерлар мижозлар деб аталади. Бу атамалар компьютер – сервер ва компьютер-мижозларда ишлатиладиган дастурий таъминотга ҳам тааллукли.

Қуйида оммавий Internet сервисларини қисқача кўриб чиқамиз.

World Wide Web (WWW) Internet даги энг кенг тарқалган, оммавий сервис ҳисобланади. Internet ўхшаб WWW сервисининг ҳам эгаси йўқ, аммо ҳар бир WWW серверга ахборотни жойлаштиришга жавобгар одамлар ёки ташкилотлар ҳамда дастурлар ва асбоб–ускуналарнинг ишлашини таъминловчи сервер маъмурлари мавжуд.

WWW сервиси Internet даги гиперматнли хужжатларни тарқатиш учун фойдаланади. *Гипертатн* – белги сўзлари (командалари) ўрнатилган матн бўлиб, бу белги сўзлари орқали бу матннинг бошқа жойига, бошқа хужжатларга, расмларга ҳавола килинади. Гиперматнли ҳавола хужжати фойдаланувчига бошқа хужжатлардаги ахборотга осонгина ўтиш имконини беради.

Фойдаланувчи гиперматнни ўқиётганида матндаги ёритилган (ажратилган) сўзни кўради. Бу сўзга курсорни тўғрилаб сичқонча тугмачаси босилса, экранда бу сўз ҳавола қилган, масалан, бу матннинг бошқа параграфи пайдо бўлади. WWW да таянч сўзлар бўйича бошқа

хужжатнинг бутунлай бошқа матнига тушиб қолиш, қандайдир дастурга кириш, маълум харакатларни бажариш мумкин.

Шундай қилиб, фойдаланувчилар хужжат матнидаги ажратилган сўзлар, тасвирлар ва график элементларини танлаб, исталган йуналишда кўчишлари ва очиқ-ойдин ўзларини қизиқтирган хужжатларга сакраб ўтишлари мумкин (хужжатнинг қаерда жойлашишидан катьий назар).

World Wide Web даги ахборотдан фойдаланишда мижоз компьютерларида *браузер* (browser) деб аталувчи махсус дастурий таъминот ишлатилади. Бу илова фойдаланувчига асосан World Wide Web серверлари тавсия этган Internet нинг турли-туман маълумотлари бўйича кўчишига имкон беради. Хозирда Microsoft Internet Explorer ва Netscape Navigator браузерлари оммавий тус олган.

Гиперматнли файллар махсус *гиперматнни белгиловчи тил* HTML (Hyper Text Mark-up Language) ёрдамида ёзилади. Таъкидлаш лозимки, тасвирлар ва бошқа номатн ташкил этувчилари хужжат матнига жойлаштирилмайди, балки алоҳида сақланади. Бунинг ўрнига хужжат матнига зарур ташкил этувчи файл номини кўрсатувчи ҳавола жойлаштирилади. 1998 йили хужжатнинг маъноли мазмунини ҳам таъсифловчи *белгилашнинг кенгайтирилган тили* стандарти XML (Extended Mark-up Language) қабул қилинди. Замонавий браузерлар хужжатларни XML ва HTML форматларида укийди.

Гиперматнлар муҳарририга эга бўлиб, ишчи муҳитнинг исталган тузилмасини, шу жумладан хужжатларни, файлларни, маълумотларни, тасвирларни, дастурий таъминотни ва ҳ. яратиш мумкин ва бу янги дастурий таъминот эмас, балки оддий гиперматн бўлади. WWW сервиси ахборотни йиғиш, тарқатиш ва ўрганиш жиҳатидан чегараланмаган имкониятга эга. Улар таъминлайдиган график воситалар фойдаланувчилар ва компаниялар орасида борган сари шухрат қозоняпти.

Ҳар қандай компания Internetга бир ёки бир нечта серверни улаб ўзининг Web-узелини яратиши мумкин. Бундай компаниялар хужжатларини World Wide Web га жойлаштириш имкониятига эга бўладилар ва бу хужжатлардан браузери бўлган ҳар қандай Internet фойдаланувчиси фойдала-

ниши мумкин. World Wide Web тавсия этадиган маркетинг имкониятларидан фойдаланишга бошлаган компаниялар бу хизматнинг реклама ва маҳсулотни сотишда ғоят катта афзалликларга эга эканлигини тушуна бошлайдилар.

WWW сервиси фойдаланувчига нафақат статик мазмунли хужжатларни кўрсатишга қодир. HTML-хужжатларда фойдаланувчи тўлдирадиган ва серверга қайтариладиган шакллар бўлиши мумкин. Шакл тўлдирилишида фойдаланувчи тақдим этилган муълумотларга боғлиқ ҳолда сервер динамик тарзда "дарҳол" жавоб хужжатини шакллантиради ва қандайдир қўшимча ҳаракатларни бажаради масалан, кредит варақасидан пулни олади, авиачиптани брон қилади, ёки хабарни фойдаланувчи кўрсатган пейджерга юборади. Тавсиф этилган технология асосида кўпгина Internet-магазинлар маълумот берадиган хизматлар, талабнома берадиган тизимлар ва ҳ. яратилади.

WWW, браузерлар ва бу хизматда ишлатилувчи "мижоз-сервер" моделининг пайдо бўлиши билан татбиқий дастур яратувчилари универсал интерфейс ва тармоқ технологияларига эга бўлдилар.

Энди ахборот тизимини яратиш учун керакли шаклларни ёзиш ва бу шаклларни фойдаланувчилар томонидан тўлдирилишига сервер реакциясини дастурлаштириш талаб этилади. Мижоз компьютерида фақат WWW – браузер ишлатилади, яъни тизим билан ишлашда ҳеч қандай қўшимча дастурий таъминот ўрнатилиши талаб этилмайди. Бундай тизим *Web-интерфейсли* тизим деб аталади. Шаклларни ишлашга қўшимча ҳолда WWW браузерга сервердан дастурни юклаш ва уни фойдаланувчи компьютерида бажариш имконини беради. Бундай дастурлар Java ва Java Script тилларида ёзилади ва Web-интерфейсни бойитади. Аммо бундай дастурларнинг бажарилиши сезиларли ҳисоблаш ресурсларини талаб этиши мумкин ва доимо хавфсизлик нуқтаи назаридан бенуқсон бўлавермайди.

Доменли исмлар сервиси DNS. Internet даги ҳар бир компьютер, у билан тармоқдаги бошқа компьютернинг уланишига имкон берувчи ўзининг шахсий ягона адресига эга бўлиши шарт. Internet даги компьютер адреслар (улар IP-адреслар деб юритишади) икки хил ёзув шаклига эга: рақамли адрес ва доменли исм. Доменли исмлар сервиси DNS бошқа сервислар томо-

нидан компьютернинг доменли исмини рақамли IP адресга трансляцияси учун ишлатилади.

Рақамли IP-адрес компьютернинг 32 битли идентификатори бўлиб, ҳар бири 8 битдан иборат 4 октетга бўлинади. Ҳар бир октет ўнли саноқ системасида ёзилиб, октетлар қиймати нуқталар орқали ажратилади. Рақамли IP-адресга мисол 184.94.125.53 адреснинг рақамли шакли компьютерларда ва тармоқ хизматининг махсус асбоб-ускуналарида ишлатилади. Одамлар учун рақамли адрес ноқулай, эсда қолиши қийин ва кам маъноли ахборотни элтади.

Одамлар одатда *доменли адреслардан* фойдаланишади, бунинг устига ҳар бир доменли исм, рақамли IP-адрес каби Internet даги фақат битта компьютерни аниқлайди. Доменли исм нуқталар билан ажратилган бир неча сўз ёки қисқартиришлардан иборат, масалан dot.msk.ru. Доменли исм компьютер макони хусусидаги фойдали ахборотни элтади. Исмнинг четки ўнг қисми юқори сатҳ доменини, яъни ушбу компьютер жойлашган компьютерларнинг катта гуруҳини билдиради. Бизнинг мисолда бу ru-Russia, Россия сўзининг қисқартирилгани. Бу юқори сатх домени Россияда Internet га уланган компьютерларни бирлаштиради. ru доменининг ичида қисм доменлар кичикроқ ўлчамли минтақа бор, масалан msk.ru(Москва). Доменли исмнинг четки чап қисми қисм доменининг ичидаги компьютер исмини билдиради (dot).

Доменли исм ҳар доим ҳам уч қисмдан иборат бўлмайди. Аммо, ҳар қандай ҳолда четки ўнг қисм юқори сатҳ доменини, четки чап қисми, компьютернинг ўз исмини, қолганлари, ўнгдан чапга-бири иккинчисига солинган ва ҳар бир кейингиси олдингисининг қисми бўлган қисм доменларни билдиради.

Юқори сатҳ доменлари икки хил бўлади. Биринси мамлакат номининг икки ҳарфли қисқартирилишидан иборат, масалан ru-Россия (Russia), fr-Франция (France), uz-Ўзбекистон (Uzbekistan) ва ҳ. Барча қисқартиришлар стандарт ҳисобланади ва Халқаро стандартлаштириш ташкилоти (ISO) томонидан аниқланган. Иккинчи хил юқори сатҳ доменлари-умумий доменлар - "машғулот тури" бўйича уч ҳарфли белгига эга.

2.1-жадвалда юқори сатх умумий доменларининг тарқалган белгиланиш рўйхати келтирилган.

2.1-жадвал

Доменнинг белгиси	Ташкилот тури
com	Тижорат ташкилотлари (масалан, www.ibm.com)
edu	Олий ўқув юртлари тармоғи (масалан, strawb.mit.edu)
gov	Ҳукумат ташкилотлари (масалан, whitehouse.gov)
org	Бошқа организациялар (масалан, isoc.org)
net	Тармоқ ишлашга тааллуқли Internet провайдерлари ва бошқа ташкилотлар. (масалан, Uznet.net)
int	Ҳалқаро ташкилотлар, масалан www.nato.int

Домен исмини рақамли IP-адресга ўзгартириш Internet нинг махсус сервери ёрдамида амалга оширилади. Бу сервер доменли исм тизими (Domain Name System) деб аталади. Бундай ўзгартирувчиларни бажарувчи компьютерлар DNS-серверлар деб аталади. Ҳар бир доменда унга хизмат қилувчи DNS-сервер мавжуд.

Файл архивларидан фойдаланиш. Internet да кўпгина серверлар файл архивларидан ошкора фойдаланишга таклиф этади. Архив тематик каталогларнинг оддий дарахти бўлиб, каталогларда асосан дастурий таъминотнинг, хужжатларнинг, китоблар матнининг ва ҳ. зичлаштирилган файллари сақланади. Файлли архифлардан турли платформа ва операцион тизимлар учун дастурий таъминотни топиш мумкин. Сервердан файлларни фойдаланувчи компьютерга жўнатиш FTP протоколи (File Transfer Protocol) ёрдамида амалга оширилади.

Аксарият мижоз дастурий воситаларига компьютерлар учун FTP билан ишлаш учун махсус дастурлар киритилган, масалан Windows операцион тизими томонидан таъминланадиган ftp.exe дастури. Бу дастур протоколнинг барча имкониятларини, жумладан парол бўйича фойдаланишни ва масофадаги компьютер файллари билан ишлаш бўйича амалларнинг тўлиқ тўпламини амалга оширади. Одатда ошкора архивлардан оддий фойдаланувчиси учун архивдан аноним фойдаланиш ва у ёки бу файлни ўз компьютерига узатиш имкониятига эга бўлиши етарли.

Ҳар қандай WWW-браузер ошкора FTP архивлардан аноним фойдаланиш учун қулай ва тушунарли интерфейсга эга.

FTP-сервер билан боғланиш ўрнатилганидан сўнг браузер дарчасида файл тизимининг каталоглар ва файллар кўринишидаги оддий тасвири пайдо бўлади. Каталогга сичқонча тугмачасининг босилиши ушбу каталогга ўтишга, файлга сичқонча тугмачасининг босилиши эса файлнинг фойдаланувчи компьютерига юкланишига олиб келади.

Электрон почта - компьютер тармоқларида амалга оширилган хизматнинг дастлабки сервисларидан бири бўлиб, фойдаланувчиларга электрон хабарларни юбориш ва қабул қилиш имкониятини беради.

Фойдаланувчи электрон почта орқали хабарларни юбориши, уларни ўзининг электрон почта қутисида олиши, мухбирлари хатига уларнинг адреслари бўйича автоматик тарзда жавоб бериши, хатининг нусхаларини бирданига бир неча қабул қилувчиларга тарқатиши, олинган хатни бошқа адресга жўнатиши, турли хат-хабарлар учун почта қутисининг бир неча бўлимларини тузиши, хатга матнли файлларни киритиши ва х. мумкин.

Электрон почта корпоратив интра-тармоқда жуда маъсулиятли вазифани бажаради. У ходимлар ўртасидаги алоқанинг ўз вақтидалигини таъминлайди ва хизмат муолажаларини тезлаштиради. Электрон почтанинг хабарларга файлларнинг киритиши имконияти, ходимларга хар кандай ахборотни - оддий ҳисоботдан то янгиланган дастурий таъминот ва тўлақонли мультимедиа тақдимотини тарқатишига имкон беради.

Кўпгина компаниялар ўзларнинг электрон почта тизимларини Internetга тарқатиш орқали кенгайтирадилар. Глобал электрон қути компаниянинг географик тарқоқ бўлимлари ва филиалларини бир-бири билан боғлаб, уларнинг ходимларига марказий офис хизматлари билан осонгига ахборот алмашиш имконини беради.

Электрон почтани компанияни унинг мобил фойдаланувчилари билан алоқасини ташкил этишда қўллаш қулай хисобланади. Компания бутун мамлакат бўйича тармоқга кириш нуқталарини таъминловчи Internet хизмати провайдерларининг тақдим қилганларидан ҳам фойдаланиши мумкин.

Электрон почта буюртмачилар ва таъминловчилар алоқаси самарадорлигини оширади. Хабарлар ва хужжатларнинг электрон форматда узатилиши қўшимча афзаллик тўғдиради, яъни қабул қилувчи бундай маълумотларни осонгина ўзгартириши ва исталган мақсадда ишлатиши мумкин.

Internetда электрон почта билан ишлаш учун TCP/IPга асосланган SMTP, POP ёки IMAP тадбиқий протоколлар ишлатилади.

Почтани узатувчи оддий протокол SMTP (Simple Mail Transfer Protocol) Internet почта серверлари ўртасида хабарлар узатишни бажаради. SMTP хабар нусхаларини турли адреслар бўйича узатиш учун кўпайтиришга ва шу тариқа тарқатиш рўйхатини шакллантиришга имкон беради. Почта сервери маълум доменли исмга юборилаётган барча хабарларнинг қабул қилинишига жавобгардир. Ҳар бир фойдаланувчи (почта қутиси) учун серверда махсус файл ажратилади ва бу файлга келадиган хабарларни, қачон фойдаланувчи уларни олиш учун сервер билан боғланишини кутган ҳолда, жойлаштирилади.

Сервер адресатларига унинг фойдаланувчиларидан келган хабарларни ҳам тарқатади. Олдиндан у DNS' хизматидан қайси сервер адресатнинг доменли исмига жавобгар эканлигини аниқлайди, сўнгра бу сервер билан SMTP протоколи бўйича алоқа ўрнатади.

POP почта протоколи (Post Office Protocol) фойдаланувчига унга келган электрон хабарлардан фойдаланишга, яъни фойдаланувчи компьютери ва фойдаланувчи почта қутиси рўйхатга олинган почта сервери билан алоқа ўрнатилишига имкон беради. Техника нуқтаи назаридан фойдаланувчи почтани олиш учун қайси компьютердан ўзининг сервери билан боғланиши ва бу компьютер сервердан қандай узоқ масофада жойлашганлиги аҳамиятли эмас. Фақат, фойдаланувчи компьютери Internetга уланган ва унда POP протоколини таъминловчи почта дастури ўрнатилган бўлиши лозим.

Фойдаланувчининг почта серверидан фойдаланишида *IMAP протоколи* ҳам ишлатилади. Бу протокол мураккаброқ бўлиб, фойдаланувчига почтани бевосита серверда каталоглашга ва сақлашга имкон беради.

Замонавий электрон почта нафақат хабарларни, балки хабарга қўшилган ихтиёрий мазмунли ва форматли бир неча файлларни (attachments) узатиш қобилиятига эга. Бундай хатлар SMTP ва POP-3 протоколлари ёрдамида одатдагидек қабул қилинади, почта серверларида ишланади ва Internet оркали узатилади.

Шуни эсдан чиқармаслик лозимки, электрон почта катта ҳажмли хабарларни узатишга мўлжалланмаган ва кўпгина серверлар қабул қилинувчи ва жўнатилувчи хабарлар ҳажмини мажбуран бир неча мегабайтларга чегаралайди.

Телеанжуманлар ва тарқатиш хизматлари. Телеанжуман хизмати ёки тармок янгиликлари (Usenet news) ошкора (бутун дунё ёки регионал) эълонлар тахтаси бўлиб, унда ҳар бир киши хабар жўнатиши ва хар бир киши бошқалар жўнатган хабарларни ўқиши мумкин. Бу хабарлар тамомила турли характерга эга ва муайян одамга эмас, балки кенг оммага адресланган. Моҳияти бўйича, Usenet-жамоа (очиқ) мунозара клубларидир.

Фойдаланишнинг қўлайлигини таъминлаш мақсадида мавзулар «қизиқишлар» бўйича алоҳида гурухларга ажратиш қабул қилинган ва бу алоҳида гурухлар анжуманлар деб юритилади.

Гуруҳларга ажратиш иерархик (шажаравий), масалан :

- comp.languages- умуман дастурлаш тилларига бағишланган гурух;
- comp.languages. c. – C дастурлаш тилига бағишланган гурух;
- comp.languages. c. libraries - C тили библиотекасига бағишланган гурух.

Бутун дунё янгиликлар гурухининг жами бир неча мингга тенг ва улар бўлиши мумкин бўлган барча натижаларни қамраб олганлар. Регионал тарқатилувчи янгиликлар гуруҳи ҳам мавжуд.

Телеанжуманлар махсус серверлар тармоғи бўйича тарқатилиб ҳар бир сервер тармоқ янгиликларини узатувчи протокол NNTP (Network News Transfer Protocol) ёрдамида мижозларнинг маълум бир сонига хизмат кўрсатади.

Телеанжуман хизматидан фойдаланиш учун фойдаланувчи компьютерига хизмат курсатувчи янгиликлар сервери бўлиши лозим. Бундай сервер

адресини провайдердан ёки тармоқ маъмуридан бўлиш мумкин. Мижоздастурлар телеанжуманлардан фойдаланиш учун WWW- броузерларига (Netcape) ёки почта дастурларига (MS Outlook Express) интеграциаланган, мустақил иловалар ҳам мавжуд. Махсус почта серверлари томонидан бажариладиган электрон почта буйича таркатиладиган хабарларнинг тематик рўйхатлари телеанжуманларга ўхшаш. Махсус почта серверларининг энг йириги Россияда-Subseribe.ru. Қандайдир тарқатишга ёзилиш учун ушбу адрес буйича ўз браузерини юбориш лозим.

Шундай тарқатишлар ҳам мавжудки, уларга хабарларни факат бошқарувчи жўнатиши мумкин ва, мос ҳолда, ёзилувчилар фақат бошқарувчига жавоб беришлари мумкин. Яна бошқа таркатиш тури- «купчиликдан купчиликка» мавжуд, яъни ҳар қандай ёзилувчи барча рўйхатга хабарни жўнатиши мумкин.

Internetда мулоқот хизматлари. ICQ хизмати. ICQ (Intelligent Call Query) хизмати номини кўпинча “I seek you” (Мен сени кидираяпман) сўзи билан боғлашади. Бу хусусий хизмат хозирда AOL Time Warner (АҚШ) компаниясига тегишли бўлиб, 1997 йилнинг бошида пайдо бўлган ва ўн миллионлаб фойдаланувчиларига эга. Бундай хизмат Microsoft (Microsoft Instant Messenger) фирмаси томонидан ҳам кўрсатилади. Internet дан фойдаланувчи ўзининг компьютерига, рўйхатдан ўтишига ва сўнгра ушбу хизмат билан ишлашига имкон берувчи, ICQ – мижозни ўрнатиши мумкин. Рўйхатдан ўтишда фойдаланувчига идентификацион номери берилади ва сўнгра у қуйидаги хизматлардан фойдалана олади.

- ICQ номерига эга бўлган Internetдан фойдаланувчиларга вақтнинг реал режимида хабарларни жўнатиш (пейджерга ўхшаш);

- сухбат куриш мумкин бўлган ICQ фойдаланувчилари билан чат (chat-ингилизча “сўзлаш ”маъносини беради);

- бошқа фойдаланувчига файлларни жўнатиш ва бошқалар.

IRC хизмати. IRC (Internet Relay Chat) хизмати кўпгина одамларнинг вақтнинг реал режимида (клавиатурада хабарларни териш йули билан) сухбат қуришларига имкон беради.

Умумий чалкашликларни олдини олиш максадида сухбатдошлар мухокаманинг турли мавзуларини таъминловчи каналларга бирлаштирилади. IRC каналларига уланиш учун *mirc* ёки *pirck* каби махсус мижоз-дастур талаб килинади. Каналларнинг барча номлари фунт белгиси «#» билан бошланади. Масалан, #hottub қидириш ва сухбат учун оммавий канал ҳисобланади. Баъзи мижоз-дастурлар бир неча каналга бир вақтнинг ўзида боғланишга имкон беради.

IRC дастури дарчасига киритган қандайдир хабарингиз бирор вақтдан сўнг каналингизнинг бошқа қатнашчилари экранида пайдо бўлади ва худди шундай, сизнинг IRC серверингизга уланган бошқа IRC фойдаланувчилари киритган хабар сизнинг экранингизда акслантирилади.

Web-интерфейсли чат серверлар («сўзлашув» серверлари) тарқалди. Чат-серверлар дастурий таъминот ўрнатилган WWW - серверлар бўлиб, бу дастурий таъминот бу серверга уланган фойдаланувчиларга оддий браузер ёрдамида бир-бирларига вақтнинг реал режимида хабарлар жунатишга имкон беради. Моҳияти билан бу сервис IRCга ўхшайди, аммо ундан фойдаланиш учун оддий браузер бўлиши кифоя.

Telnet сервиси масофадаги компьютерда дастурни бажаришга мўлжалланган. Telnet дастури ёрдами фойдаланувчи бошқа компьютерда «дарча» очади: у худди масофадаги компьютер клавиатураси олдида ўтирганидек командаларни киритиши, дастурни ишга тушириши ва унинг бажарилиши натижаларини кузатиши мумкин. Бу хизматдан ОС UNIX билан ишлайдиганлар кўпдан бери фойдаланадилар. Терминал фойдаланиш имконияти энди Windows 2000 операцион тизимининг версиясида хам пайдо бўлди.

Internetда ахборотни қидириш. Internet да, хусусан, WWW да ахборотни қидирув серверлари ёдрамида амалга оширилади. Бу серверлар вақти-вақти билан Internetдаги WWW-хужжатлар мазмунини сканерлаб, у ёки бу ахборотли хужжатларга ҳаволаларни топишга имкон берувчи маълумотлар базасини тузади. Россияда энг машхур қидирув серверлари - Яндекс (www.yandex.ru) ва Рамблер (www.rambler.ru), «катта» Internetда-www.google.com, www.altavista.com ва www.yahoo.com.

Қидирув серверлари билан ўзаро харакат оддий www- браузер оркали амалга оширилади. Одатда, қидирув сервери икки хил усулни мададлайди: *таянч сўзлар бўйича ва иерархик (шажара) классификатори бўйича*.

Таянч сўзлар бўйича қидирувни амалга ошириш учун фойдаланувчи қидирув сохасини иложи борича аникроқ белгиловчи бир неча сўзни ифодалаши лозим. Сўнгра, у бу сўзларни қидирув сервери тақдим этган шаклга киритиб, қидирув тугмачасини босади. Сервер сўровни қабул қилиб, кўрсатилган сўзлар бўлган хужжатларни қидириш мақсадида ўзининг маълумотлар базасини сканерлайди ва топилган хужжатларга хаволалар рўйхатини қайтаради. Одатда, хужжатлар таянч сўзлар мухимлигининг пасайиши тартибида сараланган. Ҳавола билан бирга хужжат мазмунининг аннотацияси ёки унинг биринчи қатори чиқарилади. Бу эса фойдаланувчига хужжатнинг керак ёки керак эмаслигини баҳолашга имкон беради. Фойдаланувчи исталган ҳавола бўйича сичқонча тугмачасини босиб, ўзини қизиктирган хужжатни бутунлай кўриб чиқиши мумкин.

Кўпгина қидирув серверлари табиий тилга қўшимча ВА, ЁКИ, ЭМАС операторлари бўлган ва қизиқтираётган сўзлар орасидаги жоиз масофани кўрсатадиган сўровларнинг расмий мантиқий тилини мададлайди.

Иерархик(шажара) классификатори бўйича қидирувга асосан исталган натижага етишмагунча, олдин рўйхатдаги ахборотнинг катта бўлишини, сўнгра унинг бўлинмасини ва ҳ. танлаш амалга оширилади. Ҳар бир қадамда фойдаланувчи тематикаси берилган бўлимга мос келувчи хужжатларга илова рўйхатини ёки унинг бўлинмалари рўйхатини кўриб туради. Масалан:Фан→Криптография→Асимметрик криптотизмлар→Рақамли имзо. У ёки бу қидирув усулини қўллаш муайян масала орқали аниқланади.

Қидирувнинг яна бошқа усулларидан FTP – серверларда архивларни кўриб чиқиш, телеанжуманлар ва тарқатишлардан фойдаланилади. Одатда файлли архивлар иерархик (шажара) классификаторларига ўхшаб тузилмаланган бўлади. Энг катта архивлардан бири ftp://ftp.funet.fi/ адреси бўйича жойлашган. Тематик телеанжуманлар ва тарқатишларга қандайдир тривиал бўлмаган масалани тушунтирувчи фойдали ахборотни ёки тажрибали мутахассислар тавсиларини топиш мумкин.

2.2. Электрон бизнес ва тижорат моделлари

Электрон бизнесни кўпинча учинчи минг йилнинг технологияси деб аташади. Internet да электрон бизнеснинг ривожи 1995 йилдан, тармоқни хусусий фойдаланувчилар томонидан ўзлаштира бошлашларидан бошланган. Худди шу йили биринчилардан бўлган Amazon-Internet магазини очилган.

Баъзида электрон бизнес ва электрон тижорат тушунчаларини аралаштиришади, аммо улар орасида анчагина фарқ бор:

- электрон бизнес (e-business) – фаолият самарадорлигини кўтариш мақсадида компания асосий бизнес жараёнларини Internet-технологиялардан фойдаланиб амалга оширишдир. Бошқача айтганда электрон бизнес - компаниянинг ички ва ташқи алоқаларини амалга ошириш учун глобал ахборот тармоқларидан фойдаланувчи хизмат фаолиятидир.
- электрон тижорат (e-commerce) электрон бизнеснинг муҳим таркибий қисмидир. Электрон тижорат бизнес-фаолиятининг турли шаклларини - чакана ва улгуржи савдо, маркетинг, корхоналар орасидаги битим, иловаларни арендага бери, хизматларни тақдим эти шва ҳ. қамраб олади. Бу барча хизмат амаллари электрон шаклда компьютер тармоқлари (корпоратив ёки Internet) ёрдамида амалга оширилади. Internet-тижорат электрон тижоратнинг қисми бўлиб, барча транзакциялар ва битимлар электрон усулда глобал тармоқ орқали амалга оширилади.

Янги бозор замонавий ахборот технологияларининг қўлланишига асосланган ва истеъмолчи билан оператив (онлайн режимида) алоқа қилинишига мўлжалланган. Яқин орада электрон савдо амаллари ҳар қандай бизнеснинг асосий қисми бўлиб қолади.

Internet-технологиялардан фойдаланувчи компаниялар рақибларига нисбатан афзаллика аввало масалаларини оператив ҳал қилишлари эвазига эришадилар. B2C, B2B ва P2P схемалари ҳозирда электрон бизнесни олиб боришнинг асосий моделлари ҳисобланади.

B2C (Business – to - Consumer) *"бизнес истеъмолчи" схемаси* Internet орқали хусусий кишига молларни ва хизматларни чакана сотишни ифодалайди.

B2B (Business – to - Business) *"бизнес-бизнес" схемаси* компанияларнинг бир бири билан махсус ахборот технологияларидан ва маълумотларни электрон алмашиш стандартларидан фойдаланган ҳолда ўзаро алоқасини ифодалайди.

P2P (Peer – to – Peer ёки Partner – to - Partner) *бизнес муносабатнинг "тенг-тенг" схемаси* Internetда бир хил ҳолатда бўлган шериклар ўртасидаги бизнес муносабатни ифодалайди.

B2B "бизнес-истеъмолчи" модели. Тижорат нуқтаи назаридан B2C "бизнес-истеъмолчи" модели электрон тижоратнинг энг истиқболли йўналиши ҳисобланади, чунки унинг асосини электрон чакана савдо ташкил этади. Internet орқали чакана савдо иқтисодиётнинг тез ривожланаётган соҳаси бўлиб электрон тижорат бозорининг анча-мунча улушини ташкил этади. B2C тизимларига қуйидагилар тааллуқли:

- савдо компанияларининг Web-дизайн воситалари ёрдамида расмийлаштирилган *Web-витриналар*;

- *Internet- магазинлар*, уларда, одатда, витринадан ташқари Internet орқали электрон савдо жараёнини бошқариш учун керакли бизнес – инфратузилма – back office мавжуд;

- back office лари компаниянинг савдо бизнес – жараёнлари билан тўла интеграцияланган Internet-магазинлардан иборат савдо *Internet-тизимлар*.

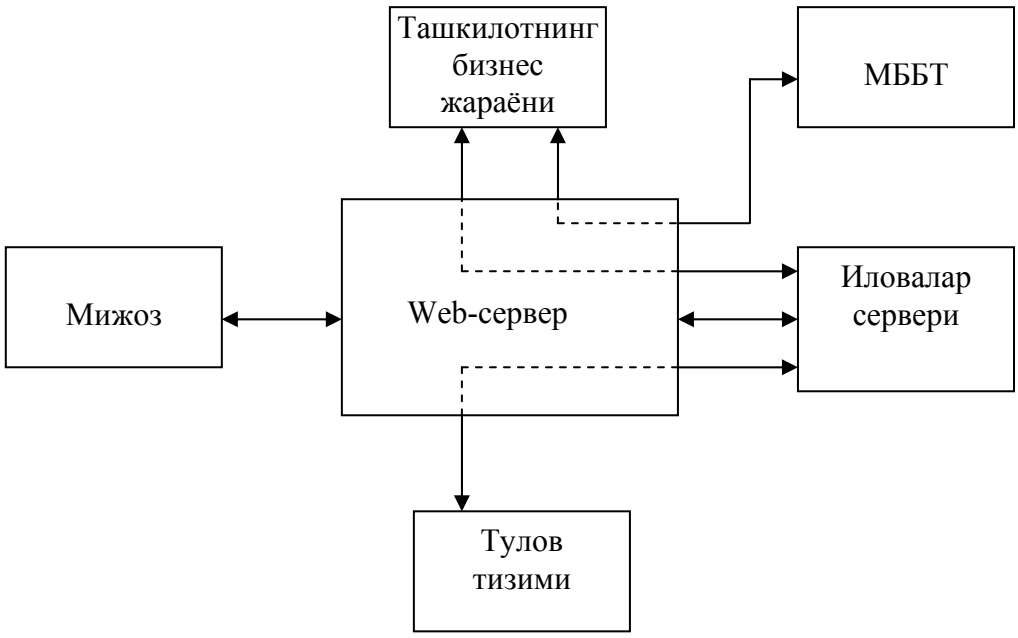
Уччало ҳолда ҳам Internet орқали савдо қилинсада, ҳар бир вариант савдо жараёнининг турли автоматлаштирилган даражасига эга. Харидорларга хизмат қилиш мураккаблиги нуқтаи назаридан турли савияга эга, савдо қилишга харажат ҳам турлича.

Web-витриналар амалга оширилишида нисбатан арзон ва етарлича оддий сайтлар ҳисобланади. Техника нуқтаи назаридан Web-витрина- каталог, навигация тизими ва буюртмани расмийлаштириш (менеджерга кейинги ишланиш учун узатилади) мажмуидир. Бошқача айтганда Web-витрина ёр-

дамида буюртмага савдо ташкил этилади. Бундай сайтларда маълум компаниянинг товарлар рўйхати (прайс-лист) онлайн каталоги кўринишида қўйилади. Таъкидлаш лозимки, Web-витринанинг рентабеллиги оддий савдо юритиш рентабеллигидан унчалик фарқ қилмайди.

Internet-магазинлар. Электрон интернет-магазинларнинг ахборот технологиялари Internet дан фойдалана олувчи харидорга уйидан чиқмасдан туриб турли фирмаларнинг товар ва хизмат навлари билан танишишга, уларнинг сифати ва нархи бўйича ахборот олишга, Internet орқали тўловни амалга оширишга ва уйга етказиб бериш билан харид қилишга имкон беради. Умумий ҳолда Internet-магазиннинг асосий вазифалари-харидорга ахборот хизматини кўрсатиш, буюртмаларни ишлаш, тўловларни амалга ошириш ҳамда турли статистик ахборотларни йиғиш ва тахлиллаш.

Internet-магазинни бошқариш схемаси 2.1-расмда келтирилган.



2.1-расм. Internet-магазинни бошқариш схемаси

Бу схемада:

- Web-сервер – тушган сўровларни тақсимлайди, фойдаланишни чегаралайди;

- иловалар сервери – барча тизим ишлашини, хусусан Internet-магазин бизнес мантиқини бошқаради;

- МББТ(маълумотлар базасини бошқариш тизими) иловалар, мижозлар, счетлар ва ҳ. хусусидаги ахборотни сақлашни ва ишлашни амалга оширади.

Талабга жавоб берадиган Internet-магазиннинг таъминоти Web-витринаникига қараганда қимматга тушсада, унинг имкониятлари жуда кенг ва рентабеллиги юқори. Ундан ташқари, ахборотнинг динамик ишланиши ва маълумотлар базасининг мавжудлиги эвазига Internet-магазин ҳар бир рўйхатдан ўтган харидор билан индивидуал ишлаш имкониятига эга.

Савдо Internet тизимлари чакана Internet савдо ривожининг юқори поғонаси ҳисобланади. Савдо Internet тизимининг Internet-магазиндан фарқи унинг сотувчининг автоматлаштирилган корпоратив тизими билан интеграцияланганидир. Бу эса компаниянинг молия-хўжалик фаолиятини оптималлаштиришга имкон беради.

Савдо Internet-тизими сотувни бевосита Internet орқали ташкил этишни мўлжаллаган ишлаб чиқарувчи компаниялар учун энг яхши танлов ҳисобланади. Бу ҳолда савдо Internet тизими сотув ахборот тизимини ишлаб-чиқариш ва етказиб бериш тизими билан боғловчи бўғин вазифасини ўтайди. Савдо Internet тизимининг ишлатилиши харажатларнинг кўпгина қисмларини, хусусан тайёр махсулотнинг катта захирасини омборга жойлаштириш харажатининг қисқаришига олиб келади.

B2B "бизнес-бизнес" модели. Бу модел компанияларнинг бир-бири билан, мос ахборот технологиялари ва маълумотларни электрон алмашиш стандартларидан фойдаланиб ўзаро электрон алоқасини ифодалайди. Корхона ва компаниялар B2Bнинг махсус виртуал майдончаси (электрон биржа) орқали ахборот алмашиш, янги партнерлар ва таъминловчиларни топиш ҳамда савдо амалларини ўтказиш имкониятига эга бўлади.

B2B-майдончанинг (электрон биржанинг) тахминий схемаси 2.2-расмда келтирилган.

Расмдан кўриниб турибдики, B2B-савдо майдончаси марказлаштирувчи Web-портал асосида истеъмолчилар ва танъминловчилар учун ечимларни бир бутунга бирлаштиради. Таъминловчилар ва истеъмолчилар сифатида йирик, ўрта ва кичик компаниялар иштирок этишлари мумкин.

2.2–расм. B2B-майдонча (электрон биржа) схемаси.

Савдо майдончасининг муайян хилига боғлиқ ҳолда майдончани яратувчилар истеъмолчиларга ёки таъминловчиларга зарур бўлган компонентларни амалга оширилишига урғу берадилар.

Internet биржалар каталоглар бўйича сотиб олиш ва сотишни, таъминлаш занжирини режалаштириш, маҳсулотни биргаликда ишлаб чиқиш, аукцион орқали савдони ва ҳ. мададлайди. Оқибат натижада Internet биржалар бизнес бўйича партнерлар алоқасини оптималлаштиришга имкон яратади ва умуман бизнес самарасини оширади.

Бизнес муносабатнинг P2P "тенг-тенг" схемаси. P2P схеманинг асосини Internet-аукционлар ташкил этади ва уларда турли товар ва хизматларни сотиб олиш/сотиш амалга оширилади. Аукционлар тармоқда савдони ташкил этувчининг сайтига ўрнатилган махсус дастурий таъминот ёрдамида ўтказилади. Internet-аукционда қатнашиш учун фойдаланувчи аукцион WWW-серверларнинг бирига аъзо бўлиши ва товар олиш (ёки ўзининг товарини сотиш учун тақдим этиш) истагини маълум қилиши лозим. Рўйхатдан ўтишга банкда электрон ҳисоб рақами бўлиши кифоя. Рўйхатдан ўтганидан сўнг фойдаланувчи ўзининг паролини айтади.

2.3. Internet орқали электрон тўловларни амалга ошириш

Internetга мўлжалланган электрон тўлов тизими Internet орқали товар ва хизматларни сотиб олиш, сотиш жараёнида молия ташкилотлари, бизнес ташкилотлари, ва Internet-фойдаланувчилари ўртасида ҳисоблашларни амалга оширувчи тизимдир. Электрон тижоратнинг ҳар қандай тизимининг иши Internetга мўлжалланган электрон тўлов тизими асосида ўзаро ҳисоблашларни амалга ошириш билан тугайди. Одатда, бу тизимлар мавжуд анъанавий тўлов тизимининг аналоглари бўлиб, асосий фарқи – бутун тўлов жараёни электрон рақам шаклда Internet имкониятларидан фойдаланган ҳолда амалга оширилади.

Айнан тўлов тизими буюртмаларни ишлаш хизматини ёки электрон витринани барча стандарт атрибутли, талабга тўла жавоб берадиган магазинга айлантиришга имкон беради. Бунда харидор сотувчининг сайтида товар ёки хизматни танлаб компьютердан узоқлашмасдан тўловни амалга ошириши мумкин.

Электрон тижорат тизимида туловлар қуйидаги қатор шартларнинг бажарилишида амалга оширилади:

- *конфиденциалликнинг сақланиши* – Internet орқали тўловлар амалга оширилишида харидор маълумотларининг (масалан, кре-

дит карта номери) фақат қонун билан белгиланган ташкилотларгина билиши кафолатланиши шарт;

- *ахборот яхлитлигининг сақланиши*-харид хусусидаги ахборот ҳеч ким томонидан ўзгартирилиши мумкин эмас;
- *аутентификация*-харидорлар ва сотувчилар иккала томон ҳам ҳақиқий эканлигига ишонч ҳосил қилишлари шарт;
- *тўлов воситаларининг қулайлиги* - харидорларга қулай бўлган ҳар қандай воситалар билан тўлов имконияти;
- *авторизация* - жараён, бу жараён кечувида транзакция ўтказилиши хусусидаги талаб тўлов тизими томонидан маъқулланади ёки рад этилади. Бу муолажа харидорнинг маблағи борлигини аниқлашга имкон беради;
- *сотувчига бўладиган хавф-хатарнинг кафолатлари* - Internetда савдо қилаётганида сотувчи товарни қайтариш ва харидорнинг инсофсизлиги билан боғлиқ кўпгина хавф-хатарга дуч келади. Хавф-хатар миқдори тўлов тизими провайдери ва савдо занжирига киритилган бошқа ташкилотлар билан махсус битим орқали келишиб олиниши шарт;
- транзакция учун тўловни минималлаштириш-буюртма ва товарга тўлов транзакцияларининг ишланиши учун тўлов, табиийки, товарнинг умумий нархига киради, демак, транзакция нархининг пасайиши фирманинг рақобатбардошлигини оширади. Таъкидлаш муҳимки транзакция учун ҳар қандай ҳолатда, ҳатто харидор товарни қайтарганда ҳам, тўланиши шарт.

Ҳозирда Internet-мўлжалланган тўлов тизимининг қуйидаги хиллари ишлатилмоқда:

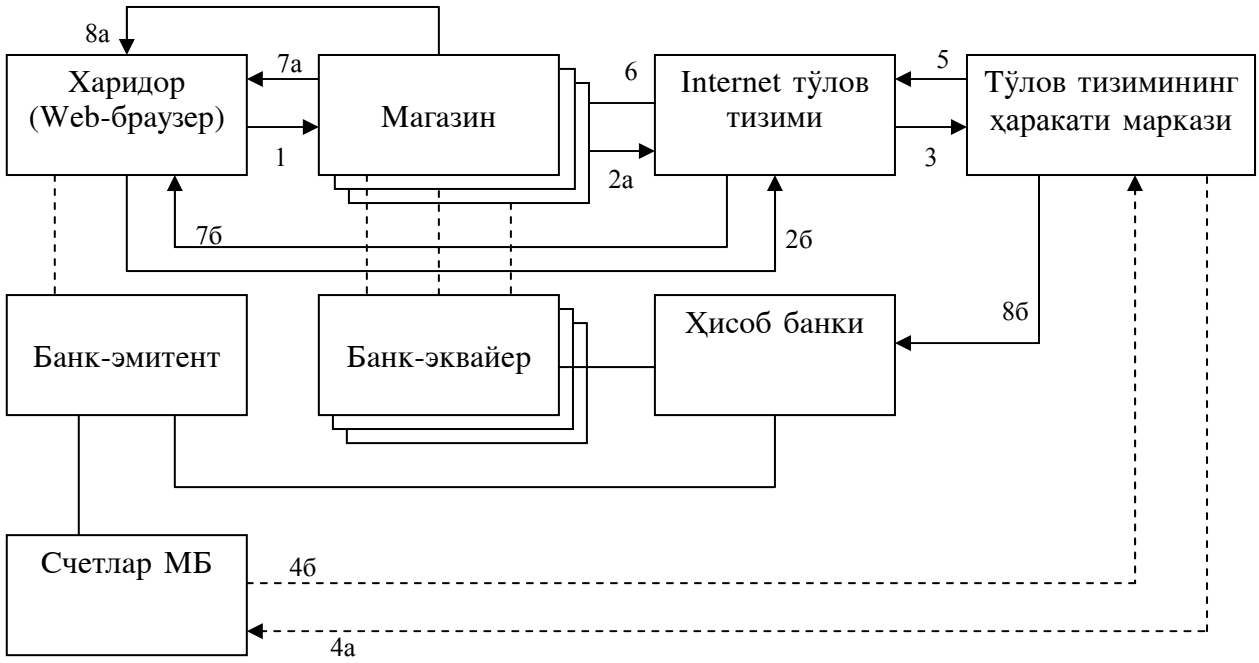
- кредитли (кредит карточкалари билан ишловчи);
- дебетли (электрон чеклар ва рақамли нақди билан ишловчи).

Кредит тизимлар. Internetга мўлжалланган тўлов тизими кредит карточкалари билан ишловчи анъанавий тўлов тизимининг аналоги ҳисобланади. Фарқи, барча транзакцияларнинг Internet орқали ўтказилиши ва натижада, ҳимоялашнинг ва аутентификациянинг қўшимча воситалари-

нинг зарурлигидадур. Кредит карточкалари мижозга банк томонидан берилган кредит ҳисобидан товарлар ва хизматларни тўлашда ишлатилади. Кредит карточкалари бўйича харид қилинганида тизим карточкани авторизациялайди ва мижознинг тўлашга қодирлигини текширади.

Ҳозирда мавжуд Internetга мўлжалланган тўлов тизимлари бир-биридан транзакцияларининг хавфсизлик даражаси ва сотувчи ва харидорга зарур бўлган дастурий таъминоти билан фарқланади.

Internetга мўлжалланган кредитли тўлов тизимининг ишлаши принципини кўрайлик (2.3-расм.)



2.3–расм. Internetга мўлжалланган кредит тўлов тизимининг умумий схемаси.

Кредит карталари ёрдамида Internet орқали тўловларни амалга оширишда қуйидагилар қатнашади:

- *харидор* – Web-браузерли компьютерга эга ва Internet дан фойдалана олувчи мижоз;
- *банк–эмитент* – бунда харидорнинг ҳисоб счети жойлашган. Банк-эмитент карточкалар чиқаради ва мижознинг молиявий мажбуриятларини бажарилишига кафил ҳисобланади;

- *сотувчилар* – товарлар ва хизматлар каталогларини олиб борувчи ва мижозлардан харидга буюртма олувчи серверлар;
- *банк-эквайерлар* – сотувчиларга хизмат кўрсатувчи банклар. Ҳар бир сотувчи ҳисоб счетини сақловчи ягона банкка эга;
- *Internetнинг тўлов тизими*-бошқа қатнашчилар ўртасида воситачи вазифасини ўтовчи электрон компонентлар;
- *анъанавий тўлов тизими* – карталарга хизмат қилувчи молиявий ва технологик воситалар;
- *тўлов тизимининг харакат маркази* – анъанавий тўлов тизими қатнашчилари ўртасида ахборот ва технологик алоқаларни таъминловчи ташкилот;
- *тўлов тизимининг ҳисоб банки* – ҳаракат марказининг топшириғи бўйича тўлов тизими қатнашчилари ўртасида ўзаро ҳисобни бажарувчи кредит ташкилот.

Тўловларни схемаси қуйидагича амалга оширилади (2.3-расмга қаралсин).

1. Харидор электрон магазинда товарлар саватини шаклланти-ради ва "кредит картаси" тўлов усулини танлайди.
2. Сўнгра кредит картасининг параметрлари (номерли, эгасининг исми, ўз кучини йўқотиш санаси) кейинги авторизациялаш учун Internetнинг тўлов тизимига узатилиши лозим. Бу амал иккита усул ёрдамида бажарилиши мумкин:
   - магазин орқали, яъни карта параметрлари бевосита магазин сайтига киритилади, сўнгра улар Internetнинг тўлов тизимига узатилади (2а);
   - тўлов тизимининг серверида (2б).

   Иккинчи йўлнинг афзаллиги равшан. Бу ҳолда карталар хусусидаги маълумот магазинда қолмайди ва, демак, унга учинчи шахснинг эга бўлиши ёки сотувчининг алдаши хавфхатари пасаяди. Иккала усулда ҳам кредит карта реквизитларини узатишда нияти бузуқ одамлар томонидан уларнинг тармоқда ушлаб қолиш имконияти мавжуд. Буни олдини

олиш учун карта тўғрисидаги маълумот шифрланиб узатилади. Демак, харидор-сотувчи, сотувчи-Internet тўлов тизими, харидор-Internet тўлов тизими алоқалари ҳимояланган протоколлар ёрдамида амалга оширилиши мақсадга мувофиқ ҳисобланади.

3. Internetнинг тўлов тизими сўровни авторизациялаш учун анъанавий тўлов тизимига узатади.
4. Кейинги қадам банк-эмитентнинг счетларининг онлайнли маълумотлар базасини олиб боришига боғлиқ. Маълумотлар базаси бўлса ҳаракат маркази картани авторизациялаш учун банк-эмитентга узатади(4а) ва сўнгра унинг натижасини олади(4б). Агар бундай база бўлмаса, ҳаракат маркази карта эгалари счетининг ҳолати тўғрисидаги маълумотни, стоп-варақаларни ўзи сақлайди ва авторизация сўровини бажаради. Бу маълумотлар банк эмитентлар томонидан мунтазам янгиланиб турилади.
5. Авторизация натижаси Internet тўлов тизимига узатилади.
6. Магазин авторизация натижасини олади.
7. Харидор авторизация натижасини магазин орқали (7а) ёки бевосита Internet тулов тизими орқали (7б) олади.
8. Авторизациянинг ижобий натижасида:

   - магазин хизмат кўрсатади ёки товар жўнатади (8а);
   - ҳаракат маркази ҳисоб банкига бажарилган транзакция хусусида ҳисоб банкига маълумот беради (8б). Харидорнинг банк-эмитентдаги счетидан магазиннинг банк-эквайеридаги счетига пул ўтказилади.

Кредит карточкали тўлов тизимининг камчиликлари сифатида қуйидагиларни кўрсатиш мумкин:

- харидор учун кредит счетини очиш зарурияти;
- карточкаларни авторизациялаш ва мижознинг тўлашга қодирлигини текшириш зарурияти транзакция ўтказишдаги чиқимларнинг ўсишига олиб келади ва бундай тизимларнинг

Internet тўлов тизимнинг мақсадли бозори бўлган микротўловларга мосланишини ёмонлаштиради;

- кредит карточкаларни тўловга қабул қилувчи магазинлар сонининг чегараланганлиги;

- анонимликнинг йўқлиги ва бунинг натижасида савдо тузилмалари томонидан сервис кўрсатилиши.

Бу хил тизимлар ичида оммавий тус олганлари – First Virtual, Open Market, Cyber Cash ва SET протоколидан фойдаланувчи тўлов тизимлари[24].

Дебет тизимлари. Дебет тўлов тизимлари чеклар ва нақд пулларнинг рақамли эквивалентларидан фойдаланишга асосланган. Тўловларнинг дебет схемалари уларнинг чекли ва оддий пулли офлайн прототипларига ухшаш қурилган. Схемада иккита мустақил томон: эмитентлар ва фойдаланувчилар иштирок этади. *Эмитент* деганда тўлов тизимини бошқарувчи субъект тушунилади. У тўлов воситаларини (масалан, банк счетларидаги пуллар) ифодаловчи қандайдир электрон бирликларни чиқаради. Тизим *фойдаланувчилари* иккита бош вазифани бажаради. Улар чиқарилган электрон бирликлардан фойдаланиб тўловларни ўтказади ва Internetга қабул қилади. Таъкидлаш муҳимки, мижоз фақат ушбу онда унинг банк счетидаги маблағга эгалик қилиши мумкин. Тўлов амаллари мижознинг молиявий активи ўлчамини камайтириш йўли билан амалга оширилади.

Электрон чеклар оддий қоғоз чекларининг аналогидир. У тўловчининг ўзининг банкидаги счетидан тўлов қабул қилувчи счетига пул ўтказиш хусусидаги фармойишидан иборат. Бу амал олувчининг банкда чекни кўрсатиши билан амалга оширилади.

Электрон чекнинг қоғоз чекдан асосий фарқи қуйидагилар:

- қоғоз чекни тўлдирганда, тўловчи ўзининг ҳақиқий имзосини қўйса, онлайн вариантида эса рақамли электрон имзо ишлатилади;

- чекларнинг ўзи электрон кўринишда берилади.

Электрон пуллар реал пулларни тўла моделлайди. Бунда эмиссион ташкилот-эмитент реал пулларнинг турли тизимларда турлича номланувчи (масалан, купонлар) электрон аналогларини чиқарадилар. Уларни фойдала-

нувчилар сотиб олиб улар ёрдамида харидлар учун тўлайдилар, сўнгра сотувчи эмитентда уларни бекор қилади. Эмиссия вақтида ҳар бир пул бирлиги бекор қилинишидан аввал уни чиқарувчи тузилма томонидан текширилади ган электрон муҳр орқали тасдиқланади.

Физик пулларнинг хусусиятларидан бири-уларниниг анонимлиги, яъни уларга қачон ва ким ишлатгани кўрсатилмайди. Баъзи тўлов тизимлари харидорга аналогия бўйича электрон нақд пулни шундай олишга имкон тўғдирадики, улар билан пул орасидаги боғлиқликни аниқлаш мумкин бўлмайди. Бу кўр имзолар деб аталувчи схемалар ёрдамида амалга оширилади.

2.4. Internet – хизматлар

Ҳозирда Internet-хизматининг қуйидаги тижорат шакллари кенг тарқалган:

- Internet-банкинг;
- Internet-трейдинг;
- Internet-суғурта;
- ASP иловаларини ижарага бериш бўйича хизмат кўрсатиш.

Internet-банкинг. Замонавий Internet-технологиялар банкларга хизматларининг бир қисмини янги савияга ўтказишга ва шу орқали янги мижозларни жалб этишга ва уларга хизмат қилиш харажатларини пасайтиришга имкон яратади. Анъанавий банкларнинг аксарияти ўз мижозларига электрон хизмат қилиш ва счет тўловининг қўшимча шаклларини тавсия этади. Фақат Internetда иш юритувчи банклар нисбатан яқинда пайдо бўлди. Улар Web-банклар деб аталади. Энг йирик Web-банклар сирасига First Internet Bank, Net-Bank, CompuBank ва қатор бошқа банклар тааллуқли.

Internet-банкинг деганда, одатда, мижозга оддий компьютер ёрдамида стандарт браузерни ишлатиб банк счетидан Internet орқали тўғридан-тўғри фойдаланиш имкониятининг берилиши тушунилади. Internet-банкинг тизимининг намунали варианти мижозларга банк офисларидаги физик шахс-

ларга (табиийки, нақд пул билан бажариладиган амаллар бундан истисно) тақдим этилувчи банк хизматининг тўлиқ тўпламини ўз ичига олади.

Ҳозирда Internet-банкинг хизмати ҳар бири Internet орқали амалга оширилувчи қуйидаги имкониятларга эга:

- нақд пулсиз ҳисоб-китобларни бажариш;
- коммунал хизматлар учун тўлови;
- Internetдан фойдаланиш учун тўлови;
- уяли ва пейджинг алоқа операторлари счетларини тўлаш;
- ички ва банклараро хужжат асосидаги тўловларни бажариш;
- ўз счетлари бўйича маблағларни ўтказиш;
- исталган вақт оралиғи учун ўз счетлари бўйича барча банк амалларини кузатиш;

Internet-банкинг тизимидан фойдаланиш мижозларга қатор имтиёзлар беради:

- фоизли ставкалари нисбатан юқори;
- шахсан банкка бориш зарурияти йўқлиги ҳисобидан мижознинг вақти жиддий тежалади;
- мижоз суткада 24 соат шахсий счетини назоратлаш ва молия бозоридаги вазиятнинг ўзгаришига тездан реакция кўрсатиш имкониятига эга.

Internet-банкинг тизимлари пластик карталар бўйича амалга ошириладиган амалларни кузатишда жуда асқотади-карта ҳисобидан маблағни чиқариш тизимлар томонидан тайёрланган ҳисоблар бўйича кўчирмада дарҳол акслантирилади. Бу мижозга ўз амалларини назоратлашда қулайлик туғдиради.

Internet-трейдинг. Internet-технологиялар фонд бозори учун жуда истиқболли. Internet-технологиялар туфайли, дунёда бўш капитални қўйишнинг энг яхши усули сифатида тан олинган қимматбаҳо қоғозларни сотиб олиш, ҳозирда барча ҳоҳловчилар учун осон. Internet-трейдинг инвесторларни битимларни тузишнинг соддалиги ва онлайн-брокерларнинг хизматига таърифларнинг пастлиги билан ўзига жалб қилади.

Internetнинг замонавий имкониятлари кўчмас мулк билан бўладиган амалларни (сотиб олиш, сотиш, алмаштириш, мерос бўйича бериш, ижара-

га бериш ва ҳ.) анъанавий шаклларига нисбатан айтарлича енгиллаштириш ва тезлаштиришга имкон беради. Мижоз уйидан чиқмасдан кўчмас мулкни сотиб олиши ва сотиши, мутахассис маслахатини олиши мумкин. Бу амалларни бажариш учун компьютери, Internetдан фойдалана олиши ва банкда счети бўлиши кифоя.

Internet-суғурта. Суғурталаш деганда суғурталанувчи-мижоз (суғурта хизматларини сотиб олувчи) билан суғурталовчи (бундай хизматларни тақдим этувчи) ўртасида шартнома муносабатларини ўрнатиш ва мададлаш тушунилади. Суғурталовчи суғурта дастурини ишлаб чиқади ва аниқлайди, мижозга таклиф этади, агар суғурталанувчи рози бўлса иккала томон шартнома тузади. Мижоз бирданига ва мунтазам тўловларни амалга оширади, суғурталовчи, ўз навбатида, сўғурта ҳолат келиши билан суғурталанувчига суғурта шартномаси шартлари бўйича компенсация пулини тўлашга мажбурият олади.

Битимга келишиш жараёнида суғурта суғурта полиси деб аталувчи хужжат шакллантирилади. Бу хужжат суғурталовчи ва суғурта компанияси учун юридик хужжат ҳисобланади. Унда суғурта объекти (мол-мулк, одам, маъсулият), суғурталанувчи ҳолат, суғурта муддатининг бошланиши ва ниҳояси, суғурта суммаси, суғурта мукофоти каби муҳим томонлари олдиндан айтиб ўтилади.

Ривожланган мамлакатлар суғурта компанияларида суғурта полисларини амалга оширувчи Internet-каналлар мавжуд.

ASP иловаларини ижарага бериш бўйича хизмат кўрсатиш. Янги иқтисодиёт ривожининг истиқболли йўналишларидан бири ASP (Applications Service Providing) иловаларини ижарага бериш бўйича хизмат кўрсатишдир. Internet ёки хусусий тармоқ орқали фойдаланувчидан узоқдаги серверда жойлашган иловалардан фойдаланишни ASP иловалари амалга оширади.

ASP иловаларининг провайдери ўзининг серверларига иловаларнинг дастурий таъминотини ўрнатади ва улардан мижозларнинг фойдаланишини таъминлайди. Мижоз компьютерига бундай дастурий таъминотни ўрнатиши, уни янгилаши, захира нусхалаши ва ҳ. шарт эмас. Барча ишларни ASP

провайдери бажаради. Мижоз провайдерга иловалардан фойдалангани учун ижара ҳақини тулайди.

Компанияларнинг ASP хизматларидан фойдаланишининг сабаби қуйидагилар.

- компания эҳтиёж сезган энг янги технологиялардан хавф-хатарсиз, катта харажатсиз ва маъмурий жавобгарсиз фойдаланиш;

- иловалардан тезда фойдаланиш зарурияти;

- агар компанияни илова қандайдир сабабларга тўла қониқтирмаса, осонгина воз кечиш имконияти.

Яқин йилларда ASP бозорининг тез ўсиши кутилмоқда. Бу эса, ўз навбатида, барча компанияларга исталган бизнес-иловалардан бир хилда фойдаланишни тақдим этиш орқали, бизнес ривожида барқарорликни таъминлайди. Аксарият аналитикларнинг фикрича, кейинчалик ASP модели бизнес иловалардан фойдаланиш усулларининг орасида устунлик қилиши мумкин.

2.5 Электрон бизнес тизими хавфсизлигининг муаммолари

Электрон бизнес харидор ва сотувчи орасидаги алоқани ташкил этиш, буюртмани ифодалаш, мухокама қилиш, ўзгартириш, товарларни ва хизматларни сотиш усулларини ҳамда тўловни амалга ошириш жараёнларини ўзгартириш учун янги технологиялардан фойдаланади. Ҳозирда электрон тижорат ва бизнеснинг аксарият муаммолари ахборот хавфсизлиги билан боғлиқ, яъни хавфсизлик муаммолари электрон тижорат ва бизнес ривожидаги жиддий тўсиқ хисобланади.

Ҳар қандай тижорат компаниясининг бошқа компаниялар билан ёки ушбу компаниянинг бўлимлари орасида алоқа ўрнатилиши зарур. Ҳозирда глобал Internet тармоғи ўзининг узеллари ўртасида ишончли ва арзон ахборот алмашинувини таъминлайди. Очиқ глобал Internet тармоғи каналларидан фаол фойдаланувчи электрон бизнеснинг ишлаши жараёнида кўпгина хавф-хатарлар пайдо бўлади.

Internetдан фойдаланиш каналлари компаниянинг ахборот ресурсларидан четдан фойдаланишга имкон бериши мумкин. Коммуникацион, хусусан HTTP – протокол асосидаги дастурлардан эхтиётсизлик билан фойдаланиш ахборот тизимининг ишга лаёқатлигини бузувчи ва/ёки ахборот тизимимаълумотларини бузувчи махсус дастур – "Троян отларининг" киришига олиб келиши мумкин. Бу хил дастурларнинг ичида вируслар энг тарқалган. Ўзига хос малакали мутахассислар корпоратив ахборот тармоқларига билинмасдан кириш учун кўпинча умуммақсад тармоқлардан фойдаланадилар.

Электрон қутисининг тез-тез ишлатилиши нияти бузуқ одамларга электрон бизнес билан шуғулланувчи ташкилот фойдаланувчилари номларини обрўсизлантиришга ёрдам бериши мумкин. Фойдаланувчилар маълумотларини (исмлар, пароллар, PIN – кодлар ва ҳ.) сақловчи тизимининг заиф жойларини қидиришдан тармоқда кенг ишлатилувчи махсус дастурлардан фойдаланиш мумкин.

Internet конфиденциал ахборотни дунёнинг исталган нуқтасига юбориши мумкин, аммо агар у етарлича химояланмаган бўлса, ушлаб қолиниши, нусхалаштирилиши, ўзгартирилиши ҳамда ҳар қандай четдаги фойдаланувчилар – нияти бузуқ одамлар, рақиблар ва оддий қизиқувчилар томонидан ўқилиши мумкин. Масалан, етарлича ҳимояланмаган тўлов топшириғи ёки кредит карточка номерини жўнатаётганда эсда тутиш лозимки, жўнатиш хусусий/шахсий тармоқ орқали амалга оширилмаяпти ва четдаги фойдаланувчилар хабарингизни манипуляция қилиш имкониятига эга. Ундан ташқари хабарингиз алмаштирилиб қўйилиши мумкин: хабарларни худди *B* фойдаланувчидан юборилганидек *A* фойдаланувчидан юбориш усуллари мавжуд. Internet тармоғи маҳсус пакет, тамомила қонуний пакетлар, сонининг хаддан ташқари кўпилги узатишдаги бузилишлар, тармоқ компонентларининг носозлиги туфайли ишга лаёқат бўлмаслиги мумкин. Бундай холлар “хизмат қилишдан воз кечиш” деб аталади ва электрон тижорат учун энг жиддий таҳдид ҳисобланади. 2.2-жадвалда ахборот хавфсизлиги бузилишининг статистикаси келтирилган[24].

2.2-Жадвал

Ахборот хавсизлиги бузилишининг турлари	**Қайд этилганлиги %**	**Йўқотишлар %**
Корпоротив тармоқдан рухсатсиз четдан фойдаланиш	44	25
Хизмат қилишдан воз кечиш	32	28
Узатишда маълумотларни алмаштириш	17	18
Фаол тинглаб кўриш	2	1
Тармоқдан рухсатсиз ички фойдаланиш	97	62
Ахборотдан рухсатсиз ички фойдаланиш	55	32

Ахборот хавфсизлиги электрон бизнес тизимининг энг мухим элементларидан бири хисобланади ва усуллар ва воситаларнинг бутун бир тўплами ёрдамида таъминланиши шарт. Электрон тижорат соҳасидаги савдо кўлами Internet хавфсизлиги масалаларидан ташвишланган харидорлар, сотувчилар ва молия институтларининг бошидан кечирувчи қўрқувлари билан чегараланади. Бу қўрқувлар, ҳусусан, қуйидагиларга асосланади:

- конфиденциалликка кафолатнинг йўқлиги- кимдир маълумотларингизни узатилаётганида ушлаб қолиши ва қийматли ахборотни (масалан, кредит карточкангизнинг номерини, товар етқазиб бериш санаси ва адрес) топишга уриниши мумкин;

- амалда иштирок этувчиларни текшириш даражасининг етарли эмаслиги - транзакция қатнашчилари текширилмаганида томонларнинг бири “маскарад” уюштириши мумкинки, унинг оқибати иккинчи томонга анча қимматга тушади. Масалан, харидор сайтга кириб ундаги компаниянинг ҳақиқийлигига шубҳа қилади, шундай ҳол ҳам рўй бериши мумкинки, харидор кредит карточкасининг номерини етарлича ваколатга эга бўлмаган шахсга беради;

- сотувчида буюртма берган харидор кредит карточкасининг қонуний эгаси эканлигинининг текшириш имкони йўқ;

- кредит карточкасининг банк–эмитенти тўловни бажаришга талаб қўйган сотувчини текширишни истаб қолиши мумкин;

- маълумотлар яхлитлигига кафолат йўқ - хатто маълумотларни жўнатувчи индентификацияланган бўлсада, учинчи томон маълумотларни, улар узатилиши вақтида, ўзгартириш имкониятига эга.

Ахборот хавфсизлигини таъминлаш нуқтаи назаридан электрон тижоратнинг намунавий қўлланилишини – Internet орқали махсулотга ва хизматларга эга бўлишни кўрайлик. Ушбу жараён қуйидаги босқичлар орқали ифодаланиши мумкин.

1. Буюртмачи Web-сервер орқали махсулот ёки хизматни танлайди ва мос буюртмани расмийлаштиради.
2. Буюртма магазиннинг буюртмалар маълумотлари банкига киритилади.
3. Буюртма берилган махсулот ёки хизматни олиш мумкинлигини маълумотларнинг марказий базаси орқали текширилади.
4. Агар маҳсулотнинг олиниши мумкин бўлмаса, буюрмачи у тўғрида огоҳлантирилади ва маҳсулот ёки хизматга эга бўлиш жараёни тўхтатилади. Маҳсулотга сўров бошқа складга (буюртмачи розилигида) йўналтирилиши мумкин.
5. Агар махсулот ёки хизмат мавжуд бўлса буюртмачи тўловни тасдиқлайди ва буюртма мос маълумотлар базасига киритилади. Электрон магазин мижозга буюртма тасдиғини юборади. Кўпгина холларда (айниқса эндигина иш бошлаган компанияларда) буюртмалар, товарларнинг борлигини текшириш ва ҳ. учун ягона маълумотлар базаси мавжуд.
6. Мижоз онлайн режимида буюртма хақини тўлайди.
7. Товар буюртмачига етқазилади.

Электрон тижорат билан шуғулланадиган компаниялар юқорида келтирилган босқичларда дуч келадиган таҳдидлар қуйидагилар:

- электрон магазин Web-сайтининг саҳифасини алмаштириб қуйиш. Бу таҳдидни амалга оширишнинг асосий усули – фойдаланувчи сўровини бошқа серверга йўллаш. Бу таҳдид олтинча босқичда буюртмачи кредит карточкасининг номерини киритганда кучаяди;

- ёлғон буюртмалар бериш ва электрон магазин ходимлари томонидан фирибгарлик қилиш. Ҳозирда ички/ташқи таҳдидлар муносабати 60/40ни ташкил этади;
- электрон тижорат тизимида узатиладиган маълумотларни ушлаб қолиш. Буюртмачининг кредит картаси хусусидаги ахборотни ушлаб қолиш ўзгача хавф-хатарни туғдиради;
- компаниянинг ички тармоғига кириш ва электрон магазин компонентларини обрўсизлантириш;
- "хизмат қилишдан воз кечиш " (denial of service) хужумини амалга ошириш ва электрон тижорат ишлашини ёки унинг узелини бузиш.

Ушбу таҳдидлар натижасида компания – электрон битим провайдери – мижозлар ишончини йўқотади, моддий зарар кўради. Баъзи холларда бу компанияларга кредит карточка номери фош қилингани учун даъво қўзғатилиши мумкин. "Хизмат қилишдан воз кечиш" хужумси натижасида электрон магазиннинг ишлаши бузилиши мумкин, унинг ишга лаёқатлигини тиклашга инсон, вақт ва материал ресурслари талаб этилади.

III боб. АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШНИНГ АСОСИЙ ЙЎЛЛАРИ

3.1. Ахборотни ҳимоялаш концепцияси

Нияти бузуқ одамларни ёлғиз фойдаланувчилар эмас, балки корпоратив компьютер тармоқлари қизиқтиради. Айнан бундай тармоқларда ахборотнинг йўолиши, рухсатсиз модификацияланиши жиддий оқибатларга олиб келиши мумкин.

Компьютер тармоқларини ҳимоялаш уйда фойдаланувчи компьютерларни ҳимоялашдан фарқланади (гарчи индивидуал ишчи станцияларни ҳимоялаш-тармоқ ҳимоясининг ажралмас қисми). Чунки, аввало, бундай масала билан саводли мутахассислар шуғулланадилар. Шу билан бирга корпоратив тармоқ хавфсизлиги тизимининг асосини четки фойдаланувчилар учун ишлаш қулайлиги ва техник мутахассиларга қуйиладиган талаблар ўртасида муросага етишиш ташкил этади.

Компьютер тизимига икки нуқтаи назардан қараш мумкин: унда фақат ишчи станциялардан фойдаланувчиларни кўриш мумкин, ёки фақат тармоқ операцион тизимининг ишлашини ҳисобга олиш мумкин.

Симлар бўйича ўтувчи ахборотли пакетлар мажмуини ҳам компьютер тармоғи дейиш мумкин. Тармоқни ифодалашнинг бир неча сатҳлари мавжуд. Худи шундай тармоқ хавфсизлиги муаммосига турли сатҳларда ёндашиш мумкин. Мос ҳолда ҳар бир сатҳ учун ҳимоялаш усули турлича бўлади. Тизимнинг ишончли ҳимояланиши ҳимояланган сатҳлар сони билан белгиланади.

Биринчи, кўриниб турган ва амалда энг қийин йўл-ходимларни тармоқ хужумларини қийинлаштирувчи хатти-ҳаракатга ўргатиш. Бу бир қарашда осондай туюлсада, аммо мушкул иш. Internet дан фойдаланишни чегаралаш лозим.

Аксарият фойдаланувчилар чегараланишлар сабабини билмайдилар. Шунинг учун тақиқилар аниқ ифодаланиши лозим.

Компьютер тармоқлари ахборотини ҳимоялашга ҳимоялаш тадбирларининг ягона сиёсатини ҳамда ҳуқуқий, ташкилий-маъмурий ва инженер-техник характерга эга чоралар тизимини ўтказиш орқали эришилади.

Тармоқда ахборотни ҳимоялашнинг зарурий даражасини ишлаб чиқишда ходимлар ва раҳбариятнинг ўзаро жавобгарлиги, шахс ва ташкилот манфаатларига риоя қилиш, ҳуқуқни муҳофаза қилувчи органлар билан ўзаро алоқа ҳисобга олинади. Рақобатли шароитда хизматларнинг катта сонини тақдим этиш ва хизмат қилиш вақтини қисқартириш орқали етакчи ўринни сақлаб қолиш ва янги мижозларни жалб этиш мумкин. Бунга фақат барча амалларни автоматлаштиришнинг зарурий даражасини таъминлаш эвазига эришиш мумкин. Айни замонда ҳисоблаш техникасининг ишлатилиши билан нафақат пайдо бўлган муаммолар ҳал этилади, балки янги ахборотни бузилиши ва йўқотилиши, тасодифан ва атайин модификацияланиши ҳамда ахборотни бегоналар тарафидан рухсатсиз олиниши билан боғлиқ ноъананавий таҳдидлар пайдо бўлади.

Мавжуд ҳолатнинг таҳлили кўрсатадики, ахборотни ҳимоялаш учун қилинадиган тадбирлар даражаси, одатда, автоматлаштириш даражасидан паст. Бундай орқада қолиш жиддий оқибатларга олиб келиши мумкин.

Автоматлаштирилган комплексларда ахборотнинг заифлигига ҳисоблаш ресурсларининг концентрацияланиши, уларнинг худудий тақсимланганлиги, магнит элтувчиларида маълумотларнинг катта ҳажмини узоқ вақт сақланиши, кўпгина фойдаланувчиларнинг ресурслардан бир вақтда фойдаланиши сабаб бўлади.

Бундай шароитда ҳимоялаш чораларини кўриш заруриятига шубҳа қилмаса бўлади. Аммо қуйидаги қийинчиликлар мавжуд:

- ҳозирги кунда ҳимояланган тизимларнинг ягона назарияси йўқ;
- ҳимоя воситаларини ишлаб чиқарувчилар хусусий масалаларни ечиш учун асосан алоҳида компонентларни тавсия этадилар, ҳимоялаш тизимини шакллантириш ва бу воситаларнинг бирга ишлатилиши масалалари эса истеъмолчи ихтиёрига қолдирилади;

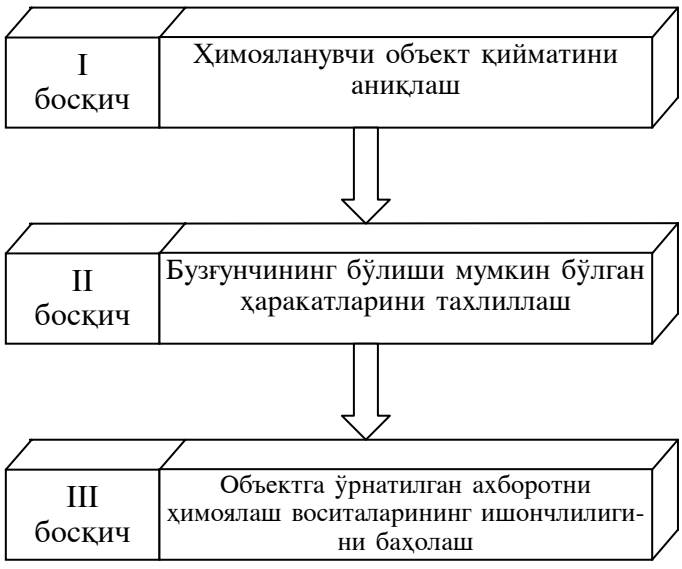
- ишончли ҳимояни таъминлаш учун техник ва ташкилий муаммолари комплексини ҳал этиш ва мос хужжатларни ишлаб чиқиш зарур.

Юқорида санаб ўтилган қийинчиликларни бартараф қилиш учун нафақат алоҳида корхона, балки давлат даражасидаги ахборот жараёнларида иштирок этувчилари ҳаракатининг координацияси зарур. Ахборот хавфсизлигини таъминлаш етарлича жиддий масала. Шунинг учун аввало ахборот хавфсизлиги концепциясини ишлаб чиқиш зарур. Концепцияда миллий ва корпоратив манфаатлар, ахборот хавфсизлигини таъминлаш принциплари ва мададлаш йўллари аниқланади ва уларни амалга ошириш бўйича масалалар таърифланади.

Концепция – ахборот хавфсизлиги муаммосига расмий қабул қилинган қарашлар тизими ва уни замонавий тенденцияларни ҳисобга олган ҳолда ечиш йўллари.

Концепцияда ифодаланган мақсадлар, масалалар ва уларни бўлиши мумкин бўлган ечиш йўллари асосида ахборот хавфсизлигини таъминлашнинг муайян режалари шакллантирилади.

Концепцияни ишлаб чиқишни уч босқичда амалга ошириш тавсия этилади (3.1-расм).



3.1–расм. Ахборот химояси концепциясини ишлаб чиқиш боскичлари

Биринчи босқичда ҳимоянинг мақсадли кўрсатмаси, яъни қандай реал бойликлар, ишлаб чиқариш жараёнлари, дастурлар, маълумотлар базаси ҳимояланиши зарурлиги аниқланиши шарт. Ушбу босқичда ҳимояланувчи алоҳида объектларни аҳамияти бўйича табақалаштириш мақсадга мувофиқ ҳисобланади.

Иккинчи босқичда ҳимояланувчи объектга нисбатан бўлиши мумкин бўлган жиноий ҳаракатлар таҳлилланиши лозим. Иқтисодий жосуслик, терроризм, саботаж, бузиш орқали ўғирлаш каби кенг тарқалган жиноятчиликларнинг реал хавф-хатарлик даражасини аниқлаш муҳим ҳисобланади. Сўнгра, нияти бузуқ одамларнинг ҳимояга муҳтож асосий объектларга нисбатан ҳаракатларининг эҳтимоллигини таҳлиллаш лозим.

Учинчи босқичнинг бош масаласи–вазиятни, хусусан ўзига хос маҳаллий шароитни, ишлаб чиқариш жараёнларини, ўрнатиб қўйилган ҳимоянинг техник воситаларини таҳлиллашдан иборат.

3.2. Ахборот ҳимоясининг стратегияси ва архитектураси

Ахборот хавфсизлиги стратегияси ва ҳимоя тизими архитектураси (3.2-расм) ахборот хавфсизлиги концепцияси асосида ишлаб чиқилади.

Ахборот хавфсизлиги бўйича тадбирлар комплексининг асосини ахборот ҳимоясининг стратегияси ташкил этиши лозим. Унда ишончли ҳимоя тизимини қуриш учун зарурий мақсадлар, мезонлар, принциплар ва муолажалар аниқланади. Яхши ишлаб чиқилган стратегияда нафақат ҳимоя даражаси, раҳналарни қидириш, брандмауэрлар ёки proxy-серверлар ўрнатиладиган жой ва ҳ. ўз аксини топиши лозим, балки ишончли ҳимояни кафолатлаш учун уларни ишлатиш муолажалари ва усуллари ҳам аниқланиши лозим.

Ахборот ҳимояси умумий стратегиясининг муҳим хусусияти хавфсизлик тизимини тадқиқлашдир. Иккита асосий йўналишни ажратиш мумкин:

- ҳимоя воситаларининг таҳлили;
- хужум бўлганини аниқлаш.

Ахборот хавфсизлигини таъминлаш иерархиясидаги иккинчи масала сиёсатни аниқлашдир. Унинг мазмуни энг рационал воситалар ва ресурслар, кўрилаётган масала мақсади ва унга ёндашиш ташкил этади. Ҳимоя сиёсати-умумий ҳужжат бўлиб, унда фойдаланиш қоидалари санаб ўтилади, сиёсатни амалга ошириш йўллари аниқланади ва ҳимоя муҳитининг базавий архитектураси тавсифланади. Бу ҳужжат матннинг бир нечта саҳифаларидан иборат бўлиб, тармоқ физик архитектурасини шакллантиради, ундаги ахборот эса ҳимоя маҳсулотини танлашни аниқлайди.

3.3. Ахборот хавфсизлигининг сиёсати

Ахборот хавфсизлигининг сиёсатини ишлаб чиқишда, аввало ҳимоя қилинувчи объект ва унинг вазифалари аниқланади. Сўнгра душманнинг бу объектга қизиқиши даражаси, ҳужумнинг эҳтимолли турлари ва кўриладиган зарар баҳоланади. Ниҳоят, мавжуд қарши таъсир воситалари етарли ҳимояни таъминламайдиган объектнинг заиф жойлари аниқланади.

Самарали ҳимоя учун ҳар бир объект мумкин бўлган таҳдидлар ва хужум турлари, махсус инструментлар, қуроллар ва портловчи моддаларнинг ишлатилиши эҳтимоллиги нуқтаи назаридан баҳоланиши зарур. Таъкидлаш лозимки, нияти бузуқ одам учун энг қимматли объект унинг эътиборини тортади ва эҳтимолли нишон бўлиб хизмат қилади ва унга қарши асосий кучлар ишлатилади. Бунда, хавфсизлик сиёсатининг ишлаб чиқилишида ечими берилган объектнинг реал ҳимоясини таъминловчи масалалар ҳисобга олиниши лозим.

Қарши таъсир воситалари ҳимоянинг тўлиқ ва эшелонланган концепциясига мос келиши шарт. Бу дегани, қарши таъсир воситаларини марказида ҳимояланувчи объект бўлган концентрик доираларда жойлаштириш лозим. Бу ҳолда душманнинг исталган объектга йўли ҳимоянинг эшелонланган тизимини кесиб ўтади. Мудофаанинг ҳар бир чегараси шундай ташкил қилинадики, қўриқлаш ходимининг жавоб чораларини кўришига етарлича вақт мобайнида хужумчини ушлаб туриш имкони бўлсин.

Сўнгги босқичда қарши таъсир воситалари қабул қилинган ҳимоя концепциясига биноан бирлаштирилади. Бутун тизим ҳаёти циклининг бошланғич ва кутилувчи умумий нархини дастлабки баҳолаш амалга оширилади.

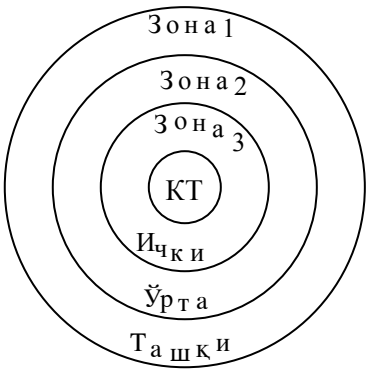
Агар бир бинонинг ичида турли ҳимоялаш талабларига эга бўлган объектлар жойлашган бўлса, бино отсекларга бўлинади. Шу тариқа умумий назоратланувчи макон ичида ички периметрлар ажратилади ва рухсатсиз фойдаланишдан ички ҳимоя воситалари яратилади. Периметр, одатда, физик тўсиқлар орқали аниқланиб, бу тўсиқлардан ўтиш электрон усул ёки қўриқлаш ходимлари томонидан бажарилувчи махсус муолажалар ёрдамида назоратланади.

Умумий чегарага ёки периметрга эга бўлган бинолар гуруҳини ҳимоялашда нафақат алоҳида объект ёки бино, балки унинг жойланиш жойи ҳам ҳисобга олиниши зарур. Кўп сонли бинолари бўлган ер участкалари хавфсизликни таъминлаш бўйича умумий ёки қисман мос келадиган талабларга эга бўлади, баъзи участкалар эса периметр бўйича тўсиққа ва ягона йўлакка эга. Умумий периметр ташкил этиб, ҳар бир бинодаги ҳимоя

воситаларини камайтириш ва уларни фақат хужум қилиниши эҳтимоли кўпроқ бўлган муҳим объектларга ўрнатиш мумкин. Худди шу тариқа участкадаги ҳар бир иморат ёки объект хужумчини ушлаб қолиш имконияти нуқтаи назаридан баҳоланади.

Юқоридаги келтирилган талаблар таҳлили кўрсатадики, уларнинг барчаси ахборотни ишлаш ва узатиш қурилмаларидан хуқуқсиз фойдаланиш, ахборот элтувчиларини ўғирлаш ва саботаж имкониятини йўл қўймасликка олиб келади.

Бинолар, иморатлар ва ахборот воситаларининг хавфсизлик тизимини назорат пунктларини бир зонадан иккинчи зонага ўтиш йўлида жойлаштирган ҳолда концентрик ҳалқа кўринишида ташкил этиш мақсадига мувофиқ ҳисобланади (3.2-расм).



1-зона. Компьютер тармоғи (КТ) хавфсизлигининг ташқи зонаси
Таъминланиши: - физик тусиқлар
- периметр бўйлаб ўтиш жойлари
- худудга кириш назоратининг ноавтоматик тизими

2- зона. КТ хавфсизлигининг ўртадаги зонаси
Таъминланиши: - эшиклари электрон ҳимояланган назорат пунктлари
- видеокузатиш
- бум буш зоналарни чиқариб ташлаш

3-зона. КТ хавфсизлигининг ички зонаси
Таъминлаш: - шахсий компьютерга фойдаланиш фақат назорат тизими орқали
- идентификациялашнинг биометрик тизими

3.3–расм. Бинодаги компьютер тизимининг хавфсизлик тизими

Ахборот хизмати бинолари ва хоналарига киришнинг назорати масаласига келсак, асосий чора-нафақат бино ва хоналарни, балки воситалар комплексини, уларнинг функционал вазифалари бўйича ажратиш ва изоляциялаш. Бино ва хоналарга киришни назоратловчи автоматик ва ноавтоматик тизимлар ишлатилади. Назорат тизими кундузи ва кечаси кузатиш воситалари билан тўлдирилиши мумкин.

Хавфсизликнинг физик воситаларини танлаш ҳимояланувчи объектнинг муҳимлигини, воситаларга кетадиган ҳаражатни ва назорат тизими ишончлилиги даражасини, ижтимоий жиҳатларни ва инсон нафси бузуқлигини олдиндан ўрганишга асосланади. Бармоқ, кафтлар, кўз тўр

пардаси, қон томирлари излари ёки нутқни аниқлаш каби биометрик индентификациялаш ишлатилиши мумкин. Шартнома асосида техник воситаларга хизмат кўрсатувчи ходимларни объектга киритишнинг махсус режими кўзда тутилган. Бу шахслар идентификацияланганларидан сўнг объектга кузатувчи ҳамроҳлигида киритилади. Ундан ташқари уларга аниқ келиш режими, маконий чегараланиш, келиб-кетиш вақти, бажарадиган иш характери ўрнатилади.

Ниҳоят, бино периметри бўйича бостириб киришни аниқловчи турли датчиклар ёрдамида комплекс кузатиш ўрнатилади. Бу датчиклар объектни қўриқлашнинг марказий пости билан боғланган ва бўлиши мумкин бўлган бостириб кириш нуқталарини, айниқса ишланмайдиган вақтларда, назорат қилади.

Вақти-вақти билан эшиклар, ромлар, том, вентиляция туйнуклари ва бошқа чиқиш йўлларининг физик ҳимояланиш ишончлилигини текшириб туриш лозим.

Ҳар бир хонага ичидаги нарсанинг муҳимлилигига боғлиқ фойдаланиш тизимига эга бўлган зона сифатида қаралади. Кириш-чиқиш хуқуқи тизими шахс ёки объект муҳимлигига боғлиқ ҳолда селекцияли ва даражалари бўйича рутбаланган бўлиши шарт. Кириш-чиқиш хуқуқи тизими марказлашган бўлиши мумкин (рухсатларни бошқариш, жадвал ва календар режаларининг режалаштирилиши, кириш-чиқиш хуқуқининг ёзма намуналари ва ҳ.).

Назорат тизимини вақти-вақти билан текшириб туриш ва уни доимо ишга лаёқатли ҳолда сақлаш лозим. Буни ихтисослашган бўлинмалар ва назорат органлари таъминлайди.

Шахсий компьютер ва физикавий ҳимоя воситалари каби ўлчамлари кичик асбоб-ускуналарни кўзда тутиш мумкин.

Юқорида келтирилганларга хулоса қилиб, компьютер тармоқларини ҳимоялашда ахборот хавфсизлиги сиёсати қандай аниқланиши хусусида сўз юритамиз. Одатда кўп сонли фойдаланувчиларга эга бўлган корпоратив компьютер тармоқлари учун махсус "Хавфсизлик сиёсати" деб аталувчи,

тармоқда ишлашни маълум тартиб ва қоидаларга бўйсиндирувчи (регламентловчи) ҳужжат тузилади.

Сиёсат одатда икки қисмдан иборат бўлади: умумий принциплар ва ишлашнинг муайян қоидалари. Умумий принциплар Internetда хавфсизликка ёндашишни аниқласа, қоидалар нима рухсат этилишини ва нима рухсат этилмаслигини белгилайди. Қоидалар муайян муолажалар ва турли қўлланмалар билан тўлдирилиши мумкин.

Одатда хавфсизлик сиёсати тармоқ асосий сервисларидан (электрон почта, WWW ва ҳ.) фойдаланишни регламентлайди ҳамда тармоқдан фойдаланувчиларни улар қандай фойдаланиш хуқуқига эга эканликлари билан таништиради. Бу эса ўз навбатида фойдаланувчиларни аутентификациялаш муолажасини аниқлайди.

Бу ҳужжатга жиддий ёндашиш лозим. Ҳимоянинг бошқа барча стратегияси хавфсизлик сиёсатининг қатъий бажарилиши тахминига асосланган. Хавфсизлик сиёсати фойдаланувчилар томонидан кўпгина маломат орттирилишига сабаб бўлади, чунки унда фойдаланувчига маън этилган нарсалар очиқ-ойдин ёзилган. Аммо хавфсизлик сиёсати расмий ҳужжат, у бир томондан Internet тақдим этувчи сервисларда ишлаш зарурияти, иккинчи томондан мос мутахассис-профессионаллар тарафидан ифодаланган хавфсизлик талаблари асосида тузилади.

Автоматлаштирилган комплекс ҳимояланган ҳисобланади, қачонки барча амаллар объектлар, ресурслар ва муолажаларни бевосита ҳимоясини таъминловчи қатъий аниқланган қоидалар бўйича бажарилса (3.4-расм).

3.4-расм. Ахборот хавфсизлиги сиёсатини таъминлашнинг асосий қоидалари.

Ҳимояга қўйиладиган талабларнинг асосини таҳдидлар рўйхати ташкил этади. Бундай талаблар ўз навбатида ҳимоянинг зарурий вазифалари ва ҳимоя воситаларини аниқлайди.

Демак, компьютер тармоғида ахборотни самарали ҳимоясини таъминлаш учун ҳимоя тизимини лойиҳалаш ва амалга ошириш уч босқичда амалга оширилиши керак.

- хавф-хатарни тахлиллаш;
- хавфсизлик сиёсатини амалга ошириш;
- хавфсизлик сиёсатини мададлаш.

Биринчи босқичда компьютер тармоғининг заиф элементлари тахлилланади, таҳдидлар аниқланади ва баҳоланади, ҳимоянинг оптимал воситалари танланади. Хавф-хатарни тахлиллаш хавфсизлик сиёсатини қабул қилиш билан тугалланади.

Иккинчи босқич – хавфсизлик сиёсатини амалга ошириш молиявий харажатларни ҳисоблаш ва масалаларни ечиш учун мос воситаларни танлаш билан бошланади. Бунда танланган воситалар ишлашининг ихтилофли эмаслиги, воситаларни етказиб берувчиларнинг обрўси, ҳимоя механизмлари ва бериладиган кафолатлар хусусидаги тўла ахборот олиш имконияти каби омиллар ҳисобга олиниши зарур. Ундан ташқари, ахборот хавфсизлиги бўйича асосий қоидалар акс эттирилган принциплар ҳисобга олиниши керак.

Учинчи босқич – хавфсизлик сиёсатини мададлаш босқичи энг муҳим ҳисобланади. Бу босқичда ўтказиладиган тадбирлар нияти бузуқ одамларнинг тармоққа бостириб киришини доимо назорат қилиб туришни, ахборот объектини ҳимоялаш тизимидаги "раҳна"ларни аниқлашни, конфиденциал маълумотлардан рухсатсиз фойдаланиш ҳолларини ҳисобга олишни талаб этади. Тармоқ хавфсизлиги сиёсатини мададлашда асосий жавобгарлик тизим маъмури бўйнида бўлади. У хавфсизликнинг муайян тизими бузилишининг барча холларига оператив муносабат билдириши, уларни тахлиллаши ва молиявий воситаларнинг максимал тежалишини ҳисобга олган ҳолда ҳимоянинг зарурий аппарат ва дастурий воситаларидан фойдаланиши шарт.

3.4. Ахборот-коммуникацион тизимлар ва тармоқлар хавфсизлигига қўйиладиган талаблар

Қўйида Россия Федарациясида ишлаб чиқилган компьютер тармоқларида ахборотни ҳимоялаш соҳасига тааллуқли ҳужжатлар хусусида сўз юритилади. Ҳужжатларда қуйилган талаблар давлат секторида ёки таркибида давлат сири бўлган ахборотни ишловчи тижорат ташкилотларида бажарилиши шарт. Бошқа тижорат тузилмалар учун ҳужжатлар тавсия характерига эга.

Ҳужжатлардан бири ахборотдан рухсатсиз фойдаланишдан ҳимоялаш бўйича талабларни акс эттиради ва "Автоматлаштирилган тизимлар. Ахборотдан рухсатсиз фойдаланишдан ҳимоялаш. Автоматлаштирилган тизимларнинг туркумланиши ва ахборотни ҳимоялаш бўйича талаблар" деб номланади.

Бу ҳужжатда хавфсизликнинг исталган даражасига эришиш бўйича асосланган чораларни ишлаб чиқиш ва қўллаш мақсадида автоматлаштирилган тизимларнинг ахборотни ҳимоялаш нуқтаи назаридан ишлаши шароитлари бўйича туркумланиши келтирилган. Ҳар бир ҳимоялаш бўйича маълум минимал талаблар мажмуи орқали характерланувчи ҳимояланишнинг тўққизта синфи белгиланади (3.1-жадвал).

3.1-жадвал. Компьютер тармоқларининг ҳимояланиш синфлари.

Талаблар	Синфлар								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
Фойдаланишни бошқариш қисм тизимига									
Идентификациялаш, ҳақиқийлигини текшириш ва субъектлар фойдаланишининг назорати									
- тизимга	х	х	х	х	х	х	х	х	х
- терминалларга, ЭҲМга, ЭҲМ тармоғи узелларига, алоқа каналларига, ЭҲМни ташқи қурилмаларига	-	-	-	х	-	х	х	х	х
- дастурларга	-	-	-	х	-	х	х	х	х
- жилдларга, каталогларга, файлларга, қайдларга	-	-	-	х	-	х	х	х	х
Ахборот оқимларини бошқариш	-	-	-	х	-	-	х	х	х
Руйхатга ва ҳисобга олиш қисм тизимига									
Рўйхатга ва ҳисобга олиш									
- субъектларнинг тизимга(дан) киришини (чиқишини)	х	х	х	х	х	х	х	х	х
- босма (график) ҳужжатларни беришни	-	х	-	х	-	х	х	х	х
- дастурни ва жараёнларни (топшириқлар, масалалар)ишга туширишни (тугаллашни)	-	х	-	х	-	х	х	х	х

- субъект дастурларидан фойдаланишни (ҳимояланувчи файллардан фойдаланиш, уларни яратиш ва йўқотиш, алоқа линиялари ва каналлари орқали узатишни)	-	-	-	x	-	x	x	x	x
- субъект дастурлариданфойдаланишни (терминаллардан, ЭҲМдан, ЭҲМ тармоғи узелларидан, алоқа каналларидан, ЭҲМ ташқи қурилмаларидан, дастурли жилдлардан, катлоглардан, файллардан, қайдлар ҳошияларидан фойдаланишни)	-	-	-	x	-	x	x	x	x
- фойдаланувчи субъектлар ваколатларини ўзгартиришларни	-	-	-	-	-	-	x	x	x
- ҳимояланувчи фойдаланиш объектнинг яратилишини	-	-	-	x	-	-	x	x	x
Ахборот элтувчиларини ҳисобга олиш	x	x	x	x	x	x	x	x	x
Оператив хотира ва ташқи тўплагичларни тозалаш	-	x	-	x	-	x	x	x	x
Ҳимояни бузишга уринишни сигнализацияси	-	-	-	-	-	x	x	x	x
Криптографик қисм тизимига									
Конфиденциал ахборотни шифрлаш	-	-	-	-	-	-	x	x	x
Фойдаланишни турли субъектларига (субъектлар гуруҳига) тегишли ахборотни турли калитларда шифрлаш	-	-	-	-	-	-	-	-	x
Аттестациядан ўтган (сертификацияланган) криптографик воситалардан фойдаланиш	-	-	-	-	-	-	-	x	x
Яхликликни таъминловчи қисм тизимига									
Дастурий воситалар ва ишланувчи ахборотнинг яхлитлигини таъминлаш	x	x	x	x	x	x	x	x	x
Ҳисоблаш техникаси воситалари ва ахборот элтувчиларини қўриқлаш	x	x	x	x	x	x	x	x	x
Ахборот ҳимояси маъмуриятининг (хизматининг) мавжудлиги	-	-	-	x	-	-	x	x	x
Ахборот ҳимояси тизимини вақти-вақти билан тестлаш	x	x	X	x	x	x	x	x	x
Ахборот ҳимояси тизимини тиклаш воситаларининг мавжудлиги	x	x	x	x	x	x	x	x	x
Сертификацияланган ҳимоя воситаларидан фойдаланиш	-	x	-	x	-	-	x	x	x

Синфлар ахборот ишланиши хусусиятлари билан бир-биридан фарқланувчи учта гуруҳга бўлинади. Ҳар бир гуруҳ ичида ахборотнинг қийматлигига (конфиденциаллигига) боғлиқ ҳолда ҳимоя бўйича талаблар иерархияси ва, демак, ҳимояланиш синфлари сақланади. Ҳар бир гуруҳ кўрсаткичларини, охиргисидан бошлаб кўриб чиқамиз.

Учинчи гуруҳ бир хил конфиденциаллик даражасига эга бўлган элтувчиларда жойлаштирилган барча ахборотдан фойдаланувчи бита фойда-

ланувчи ишлайдиган тизимлардан иборат. Гуруҳда иккита – 3Б ва 3А синфлари мавжуд.

Иккинчи гуруҳ ҳар хил конфиденциаллик даражасига эга бўлган ишланувчи ва/ёки элтувчиларда жойлаштирилган барча ахборотдан фойдаланишга бир хил хуқуқли фойдаланувчилари бўлган тизимлардан иборат. Гуруҳда иккита – 2Б ва 2А синфлари мавжуд.

Биринчи гуруҳ кўпчилик фойдаланувчи тизимлардан иборат бўлиб, уларда бир вақтнинг ўзида конфиденциаллик даражаси турли ахборот ишланади ва/ёки сақланади. Гуруҳда бешта -1Д, 1Г, 1В, 1Б ва 1А синфлари мавжуд.

Умумий ҳолда ҳимоялаш тадбирлари 4 та қисм тизимни ўз ичига олади:

- фойдаланишни бошқариш;
- рўйхатга ва ҳисобга олиш;
- криптографик;
- яхлитликни таъминлаш.

Ҳисоблаш техникаси воситаларини рухсатсиз фойдаланишдан ҳимояланиш кўрсаткичлари "Ҳисоблаш техникаси воситалари. Ахборотни рухсатсиз фойдаланишдан ҳимоялаш. Ҳимоялаш кўрсаткичлари" деб аталувчи ҳужжатда келтирилган. Унда ахборотдан рухсатсиз фойдаланишдан ҳимояланишнинг 7 синфи аниқланган. Энг пастки синф – еттинчи, энг юқори синф – биринчи. Ҳар бир синф ҳимояланиш талабларини олдингисидан мерос қилиб олади. Ҳимоянинг амалга оширилган моделлари ва уларни текшириш ишончлилигига боғлиқ ҳолда синфлар тўртта гуруҳга ажратилади.

Биринчи гуруҳда фақат еттинчи синф бўлади (минимал ҳимояланиш).

Иккинчи гуруҳ танланадиган ҳимоя билан характерланиб олтинчи ва бешинчи синфларни ўз ичига олади. Танланувчи ҳимоя номма-ном айтилган объектларнинг тизимнинг номма-ном айтилган объектлардан фойдаланишни кўзда тутади. Бунда ҳар бир "субъект-объект" жуфтлиги учун фойдаланишнинг рухсат этилган турлари аниқланиши шарт. Фойдаланиш назорати ҳар бир объектга ва ҳар бир субъектга қўлланилади.

Учинчи гуруҳ мухтор ҳуқуқли ҳимоя билан характерланиб, тўртинчи, учинчи ва иккинчи синфларни ўз ичига олади. Мухтор хуқуқли ҳимоя тизимнинг ҳар бир субъект ва объектига, унинг мос иерархиядаги ўрнини кўрсаатувчи туркумлаш белгисини бериш тизимдан фойдаланувчи ёки махсус ажратилган субъект томонидан амалга оширилади. Ушбу ҳуқуқга кирувчи синфлардан талаб қилинадиган нарса-фойдаланишнинг диспетчерини (reference monitor–ҳаволалар монитори) амалга оширилиши.

Фойдаланиш назорати барча объектларга нисбатан ҳар қандай субъект томонидан очиқ ва яширин фойдаланишда амалга оширилиши шарт. Фойдаланишга рухсат бериш фақат танланадиган ва мухтор хуқуқли қоидаларнинг биргаликда рухсати бўлгандагина амалга оширилиши мумкин.

Тўртинчи гуруҳ тасдиқланган ҳимоя билан характерланиб фақат биринчи синфни ўз ичига олади.

Тизим ҳимояланиш синфини олиши учун қуйидагиларга эга бўлиши лозим:

- тизим бўйича маъмур қўлланмаси;
- фойдаланувчи қўлланмаси;
- тестлаш ва конструкторлик хужжатлар.

Юқорида кўриб ўтилганидек, ҳозирда компьютер жиноятчилиги жуда ҳам турли-туман. Бу компьютердаги ахборотдан рухсатсиз фойдаланиш, дастурий таъминотга мантиқий бомбаларни киритиш, компьютер вирусларини ишлаб чиқиш ва тарқатиш, компьютер ахборотини ўғирлаш, дастурий-ҳисоб комплексларини ишлаб чиқишда, қуришда ва эксплуатациясида пала-партишлик.

Ахборот хавфсизлигининг бевосита таъминловчи, компьютер жиноятчилигининг олдини олувчи барча чораларни қуйидагиларга ажратиш мумкин:

- ҳуқуқий;
- ташкилий-маъмурий;
- инженер-техник.

Ҳуқуқий чораларга компьютер жиноятчилиги учун жавобгарликни белгиловчи меъёрларни ишлаб чиқиш, дастурчиларнинг муаллифлик

ҳуқуқини ҳимоялаш, жиноий ва фуқаролик қонунчилигини ҳамда суд жараёнини такомиллаштириш киради. Уларга яна компьютер тизимларини яратувчи устидан жамоатчилик назорати масалалари ҳамда, агар компьютер тизимларининг битимга келган мамлакатларнинг ҳарбий, иқтисодий ва ижтимоий жиҳатларига таъсири бўлса, чеклашлар бўйича мос ҳалқаро шартномаларни қабул қилиш киради. Фақат охирги йилларда компьютер жиноятчиликларига ҳуқуқий кураш муаммолари бўйича ишлар пайдо бўлди.

Ташкилий-маъмурий чораларга компьютер тизимларини қўриқлаш, ходимларни танлаш, махсус муҳим ишларни бир киши томонидан бажарилиши ҳолларига йўл қўймаслик, марказ ишдан чиққанида унинг ишга лаёқатлигини тиклаш режасининг мавжудлиги, барча фойдаланувчилардан (юқори раҳбарлар ҳам бунга киради) ҳимояланиш воситаларининг универсаллиги, марказ хавфсизлигини таъминлашга мутасадди шахсларга жавобгарликни юклаш, марказ жойланадиган жойни танлаш ва ҳ. киради.

Инженер-техник чораларга компьютер тизимидан рухсатсиз фойдаланишдан ҳимоялашни, муҳим компьютер тизимларни резервлаш, ўғирлаш ва диверсиядан ҳимояланишни таъминлаш резерв электр манбаи, хавфсизликнинг махсус дастурий ва аппарат воситаларини ишлаб чиқиш ва амалга ошириш ва ҳ. киради.

IV боб. АХБОРОТ ХАВФСИЗЛИГИНИНГ ХУҚУҚИЙ ВА ТАШКИЛИЙ ТАЪМИНОТИ

4.1. Ахборот хавфсизлиги сохасида хуқуқий бошқариш

Ахборот хавфсизлигининг хуқуқий таъминоти – ахборотни химоялаш тизимида бажарилиши шарт бўлган қонун чиқариш актлар, меъёрий-хуқуқий хужжатлар, қоидалар йўриқномалар, қўлланмалар мажмуи. Хозирда ахборот хавфсизлигининг хуқуқий таъминоти масаласи ҳам амалий, ҳам қонунчилик жихатидан фаол ўрганиб чиқилмоқда.

Компьютер жиноятчиликларини қилиш инструментлари сифатида телекоммуникация ва хисоблаш техникаси воситалари, дастурий таъминот ва интеллектуал билим ишлатилади. Компьютер жиноятчиликларини қилиш сохаси сифатида нафақат компьютерлар, глобал ва корпоратив тармоқлар (Internet/Intranet), балки ахборот технологиясининг замонавий, юқори унумли воситалари хамда ахборотнинг ката хажми ишланадиган, масалан, статистик ва молия институтлари, танланади.

Шу сабабли, хар қандай ташкилот фаолиятини турли- туман ахборотни олиш учун қўлда ёки хисоблаш техникаси воситалари ёрдамида ишлаш, ахборотни тахлиллаш натижасида қандайдир муйаян ечимларни олиш ва уларни алоқа каналлари орқали узатишсиз тасаввур этиб бўлмайди. Компьютерга ҳам тажовуз объекти, ҳам тажовуз қилувчи инструмент сифатида қараш мумкин. Агар компьютер фақат тажовуз обьекти бўлса, қонун бузилишини мавжуд хуқуқий меъёрлар орқали бахолаш мумкин. Агар компьютер фақат инструмент бўлса «техник воситаларни қўллаш» аломати етарли бўлади. Юқоридаги тушунчаларни бирлаштириш мумкин - компьютер бир вақтнинг ўзида ҳам инструмент ва ҳам объект. Хусусан бундай вазиятга машина ахборотининг ўғирланиши факти таалуқли.

Агар ахборотнинг ўғирланиши моддий ва маънавий бойликларнинг йўқотилиши билан боғлиқ бўлса, бу факт жиноят сифатида баҳоланади. Шунингдек агар ушбу факт билан миллий хавфсизлик, муаллифлик манфа-

атлари боғлиқ бўлса, жиноий жавобгарлик Ўзбекистон Республикаси қонунларида бевосита кўзда тутилган.

Ҳар қандай давлатда ахборот хавфсизлигининг хуқукий таъминоти халқаро ва миллий ҳуқуқий меъёрларни ўз ичига олади (4.1-расм)

4.1-расм. Ахборот хавфсизлигини таъминлашнинг хуқуқий меъёрлар

Хуқуқий бошқариш предметлари қуйидагилар.

- ахборот химоясининг хуқуқий режими;

- ахборотлаштириш жараёнларида қонуний муносабат қатнашчиларининг хуқуқий мақоми;

- субъектларнинг, уларнинг ахборот тузилмалари ва тизимлари ишлаши жараёнининг турли босқич ва сатҳларидан хуқуқий мақомиини ҳисобга олган ҳолда, муносабатлари тартиби;

Ахборот хавфсизлиги бўйича қонунларни Ўзбекистон Республикаси бутун қонунлар тизимининг ажралмас қисми сифатида тасаввур қилиш мумкин, хусусан:

- таркибида ахборотлаштириш масалаларига доир меъёрлар бўлган конституция қонунлари;

- таркибида ахборотлаштириш масалаларига доир меъёрлар бўлган умумий асосий қонунлар (мулк, ер ости бойликлари, ер, фуқоролар хуқуқи, фуқоролик, солиқ хусусида);

- хўжаликнинг алохида тузилмаларига, иқтисодиётга, давлат органлари тизимига тегишли бошқариш ва уларнинг мақомини аниқлаш бўйича қонунлар. Бу қонунлар ахборот масалалари бўйича алохида меъёрларни ўз ичига олади;

- муносабатларнинг, хўжалик соҳаларининг жараёнларнинг муайян муҳитига бутунлай тегишли махсус қонунлар. Буларга ахборотлаштириш бўйича қонунлар тааллуқли;

- ахборотлаштириш соҳасидаги қонун талабларининг бажарилишини регламентловчи меъёрий хужжатлар;

- қонунлар билан белгиланган ахборотлаштириш соҳасидаги меъёрий хужжатлар;

- таркибида ахборотлаштириш соҳасида қонун бузилишига жавобгарлик меъёрлари бўлган Ўзбекистон Республикасининг хуқуқни муҳофаза қилиш қонунлари.

Компьютер тармоқлари хавфсизлигини таъминловчи давлат хуқуқий механизмининг ривожланмаган шароитида корхонанинг давлат ва ходимлар жамоаси билан муносабатларни хуқуқий асосда ростловчи хужжатлари жиддий аҳамиятга эга бўлади. Бундай муҳим хужжатлар таркибига куйидагиларни киритиш мумкин:

- корхона (фирма, банк) устави;

- жамоа шартномаси;

- жамоа ходимлари билан тузилган, тижорат сири бўлган маълумотлар ҳимоясини таъминлаш бўйича талабларга эга мехнат шартномалари;

- ишчи ва хизматчиларнинг ички мехнат тартиб қоидалари;

- раҳбарлар, мутахассислар ва хизмат кўрсатувчи ходимларнинг мансаб билан боғланган мажбуриятлари.

4.2. Ахборот хавфсизлигининг ташкилий-маъмурий таъминоти

Ахборотни ишончли ҳимоя механизмини яратишда ташкилий тадбирлар муҳим рол ўйнайди, чунки конфиденциал ахборотлардан рухсатсиз фойдаланиш асосан, техник жиҳатлар билан эмас, балки ҳимоянинг элементар қоидаларини эътиборга олмайдиган фойдаланувчилар ва ходимларнинг жинояткорона ҳаракатлари, бепарволиги, совуққонлиги ва маъсулиятсизлиги билан боғлиқ.

Ташкилий таъминот конфиденицал ахборотдан фойдаланишга имкон бермайдиган ёки жиддий қийинчилик туғдирувчи ижрочиларнинг ишлаб-чиқариш ва ўзаро муносабатларини меъёрий-хуқуқий асосида регламентлашдир.

Ташкилий тадбирларга қуйидагилар киради:

- хизматчи ва ишлаб чиқариш бино ва хоналарни лойиҳалашда, қуришда ва жиҳозлашда амалга ошириладиган тадбирлар. Бу тадбирларнинг асосий мақсади худудга ва хоналарга яширинча кириш имконини йўқотиш; одамларнинг ва транспортнинг юриши назоратининг қулайлигини таъминлаш; фойдаланишнинг алоҳида тизимига эга бўлган ишлаб-чиқариш зоналарини яратиш ва ҳ.;

- ходимларни танлашда амалга ошириладиган тадбирлар. Бу тадбирларга ходимлар билан танишиш, конфиденциал ахборот билан ишлаш қоидалари билан ишлашни ўргатиш, ахборот ҳимояси қоидасини бузганлиги учун жавобгарлик даражаси ва ҳ. билан таништириш киради;

- ишончли пропуск режимини ва ташриф буюрувчиларнинг назоратини ташкил қилиш;

- хона ва худудларни ишончли қуриқлаш;

- хужжатлар ва конфиденциал ахборот элтувчиларини сақлаш ва ишлатиш, шу жумладан қайд этиш, бериш, бажариш ва қайтариш тартибларига риоя қилиш;

- ахборот ҳимоясини ташкил этиш, яъни муайян ишлаб чиқариш жамоаларида ахборот хавфсизлигига жавобгар шахсни тайинлаш, конфиденциал ахборот билан ишловчи ходимлар ишини мунтазам текшириб туриш.

Бундай тадбирлар ҳар бир муайян ташкилот учун ўзига хос хусусиятга эга бўлади.

Ташкилий тадбирларнинг талайгина қисмини ходимлар билан ишлаш эгаллайди. Мулкчиликнинг турли шаклларига эга бўлган корхона ходимлари билан ишлашда ташкилий тадбирлар, умумий ҳолда қуйидагиларни ўз ичига олади:

- ишга қабул қилишда суҳбат. Суҳбат натижасида номзоднинг мос бўш жойга қабул қилиниши мақсадга мувофиқлиги аниқланади;

- муайян корхонада конфиденциал ахборот билан ишлаш қоидалари ва муолажалари билан танишиш; ишга қабул қилинувчи корхона тижорат сирларини сақлаши бўйича тилхат ва фирма сирларини ошкор қилмасликка ваъда беради;

- ходимларни конфиденциал ахборот билан ишлаш қоидалари ва муолажаларига ўқитиш. Ходимларни ўқитишда нафақат ишлаб-чиқариш кўникмаларига эга бўлиш ва уларни юқори даражада сақлаш, балки уларни саноат (ишлаб чиқариш) махфийлиги ахборот хавфсизлиги, интеллектуал мулк ва тижорат сирлари ҳимояси талабларини бажариш зарурлигига қатъий ишонч руҳида тарбиялаш кўзда тутилади. Мунтазам ўқитиш раҳбарият ва ходимларнинг корхона тижорат манфаатларини ҳимоя қилиш масалалари бўйича билимдонлик даражасини ошишига имкон яратади;

- ишдан бушаётганлар билан суҳбат. Суҳбат давомида ишдан бушаётган ходимнинг фирма сирларини фош қилмасликка қатъий ваъда бериши лозимлиги таъкидланади ва бу ваъда, одатда, тилхат орқали расмийлаштиради.

Тадбирларнинг муҳим йўналишларидан бири иш юритиш ва хужжат юритиш тизимини пухта ташкил этиш ҳисобланади. Бу эса ўз иш юритиш тартибини, хужжатларни қайдлаш, ишлаш, сақлаш, йўқотиш ва мавжудлигини ҳамда тўғри бажарилишини назорат қилишни таъминлайди. Тизимни амалга оширишда хужжатлар хавфсизлигига ва ахборот конфиденциаллигига алоҳида эътибор бериш лозим.

Ахборотни хужжатлаштириш қатъий белгиланган қоидалар ёрдамида амалга оширилади. Бу қоидаларнинг асосийлари ГОСТ 6.38-90 "Ташкилий-

бошқарувчи хужжатлар тизими. Хужжатларни расмийлаштиришга талаблар", ГОСТ 6.10.4-84 "Унификацияланган хужжатлар тизими. Ҳисоблаш техника воситалари орқали яратилувчи машина элтувчиларидаги ва машинограммалардаги хужжатларга хуқуқий куч бериш" кабилар баён этилган. Бу ГОСТларда ахборотга хужжат хуқуқини берувчи 31 та реквизитлар кўзда тутилган, аммо бу реквизитларнинг барчасининг хужжатда мавжудлиги шарт эмас. Асосий реквизит – матн. Шу сабабли, ҳар қандай равон баён этилган матн хужжат ҳисобланади ва унга хуқуқий куч бериш учун сана ва имзо каби муҳим реквизитларнинг мавжудлиги кифоя.

Автоматлаштирилган ахборот тизимларидан олинган хужжатлар учун алоҳида тартиб қўлланилади. Бунда, маълум холларда, масофадан олинган ахборот электрон имзо билан тасдиқланади. Ахборотни ҳимоялаш учун барча ташкилий тадбирларни таъминловчи махсус маъмурий хизматни яратиш талаб қилинади. Унинг штат тузилмаси, сони ва таркиби фирманинг реал эҳтиёжлари, ахборотининг конфиденциаллик даражаси ва хавфсизлигининг умумий ҳолати орқали аниқланади.

Маъмурий тадбирларга қуйидагилар киради:

- операцион тизимнинг тўғри конфигурациясини мададлаш;
- иш журналларининг назорати;
- пароллар алмашишининг назорати;
- ҳимоя тизимида "раҳна"ларни аниқлаш;
- ахборотни ҳимояловчи воситаларни тестлаш.

Тармоқ операцион тизимининг тўғри конфигурациясини мададлаш масаласини, одатда, тизим маъмури ҳал этади. Маъмур операцион тизим (одамлар эмас) риоя қилиши лозим бўлган маълум қоидаларни яратади. Тизимни маъмурлаш – конфигурация файлларини тўғри тузишдир. Бу файлларда (улар бир нечта бўлиши мумкин, масалан тизимнинг ҳар бир қисмига биттадан файл) тизим ишлаши қоидаларининг тавсифи бўлади.

Хавфсизлик маъмури компьютер тармоғи ҳолатини оператив тарзда (тармоқ компьютерлари ҳимояланиши холатини кузатиш орқали) ва оператив бўлмаган тарзда (ахборот ҳимояси тизимидаги воқеаларни қайдловчи журналларни тахлиллаш орқали) назоратлаш лозим. Ишчи станциялар со-

нининг ошиши ва турли-туман компонентлари бўлган дастурий воситаларнинг ишлатилиши ахборот ҳимояси тизимидаги ходисаларни қайдлаш журналлар ҳажмини жиддий ошишига олиб келади. Журналлардаги маълумотлар ҳажми шунчалик ошиб кетиши мумкинки, маъмур улар таркибини жоиз вақт мобайнида таҳлиллай олмайди.

Тизим заифлигининг сабаби шундаки, биринчидан, фойдаланувчини аутентификациялаш тизими фойдаланувчи исмига ва унинг паролига (кўз тўридан фойдаланиш каби экзотик ҳолллар бундан мустасно), иккинчидан, фойдаланувчи тизимида тизимни маъмурлаш хуқуқи берилган супервизорнинг (supervisor) мавжудлигига асосланади. Супервизор паролини сақлаш режимининг бузилиши бутун тизимдан рухсатсиз фойдаланиш имконини яратади.

Ундан ташқари бундай қоидаларга асосланган тизим-статик, қотиб қолган тизим. У фақат қатъий маълум хужумларга қарши тўра олиши мумкин. Олдиндан кўзда тутилмаган қандайдир янги таҳдиднинг пайдо бўлишида тармоқ хужуми нафақат муваффақиятли, балки тизим учун кўринмайдиган бўлиши мумкин. Шунинг учун, муассасада ишлатилувчи ахборотнинг қайсиси ҳимояга муҳтож эканлигини аниқ тасаввур қилиш муҳим ҳисобланади. Мавжуд ахборотни тахлиллашдан бошлаш лозим. Бу муолажалар ахборот ҳимоясини таъминлаш бўйича тадбирларни дифференциаллаш имконини беради ва натижада, сарф-ҳаражатларнинг қисқаришига сабаб бўлади.

Ахборот ҳимояси тизимини эксплуатация қилиш босқичида хавфсизлик маъмурининг фаолияти фойдаланувчилар ваколатларини ўз вақтида ўзгартиришдан ҳамда тармоқ компьютерларидаги ҳимоя механизмларини созлашдан иборат бўлади. Фойдаланувчилар ваколатларини ва компьютер тармоқларида ахборотни ҳимоялаш тизимини созлашни бошқариш муаммоси, масалан, тармоқдан марказлаштирилган фойдаланиш тизимидан фойдаланиш асосида ҳал этилиши мумкин. Бундай тизимни амалга оширишда тармоқ асосий серверида ишловчи махсус фойдаланишни бошқарувчи сервердан фойдаланилади. Бу сервер марказий ҳимоя маълумотлари базасини локал ҳимоя маълумотлари базаси билан автоматик тарзда синхронлайди.

Фойдаланишни бошқаришнинг бу тизимида фойдаланувчи ваколати вақти-вақти билан ўзгартирилади ва марказий ҳимоя маълумотлари базасига киритилади, уларнинг муайян компьютерларда ўзгариши навбатдаги синхронлаш сеансида вақтида амалга оширилади.

Ундан ташқари фойдаланувчи паролини ишчи станцияларининг бирида ўзгартирса, унинг янги пароли марказий ҳимоя маълумотлари базасида автоматик тарзда аксланади, ҳамда бу фойдаланувчи ишлашига рухсат берилган ишчи станцияларга узатилади.

4.3. Ахборот хавфсизлиги бўйича стандартлар ва спецификациялар

Ахборот хавфсизлиги сохасида мутахассислар ўз фаолиятларида мос стандартлар ва снецификацияларни четлаб ўташолмайдилар. Бунга сабаб, биринчидан стандартлар ва спецификациялар – аввало ахборот хавфсизлигининг муолажавий ва дастурий-техник даражалари бўйича билимларини тўплаш шаклларидан бири. Уларда малакали мутахассислар томонидан ишлаб чиқилган, тасдиқланган юқори сифатли ечимлар ва методологиялар қайд этилган. Иккинчидан, стандартлар ва спецификациялар аппарат-дастурий тизимлар ва уларнинг компонентларининг ўзаро қўшила олишлигини таъминловчи асосий восита хисобланади. (Internet–уюшмада бу восита хақиқатдан самарали ишламоқда).

Стандартлар ва спецификацияларнинг бир-биридан жиддий фарқланувчи иккита гурухини ажратиш мумкин:

- ахборот тизимларини ва хавфсизлик талаблари бўйича химоя воситаларини баҳолаш ва туркумлаш учун аталган бахолаш стандартлари;
- химоя воситалари ва усулларини амалга ошириш ва улардан фойдаланишнинг турли жихатларини регламентловчи спецификациялар.

Бу гурухлар маълумки, ихтилофга бормайдилар, балки бир-бирини тўлирадилар. Баҳолаш стандартлари ташкилий ва архитектуравий спецификациялар вазифасини ўтаган холда ахборот тизимларининг ахборот хавфсизлиги нуқтаи назаридан мухим бўлган тушунчалари ва жихатларини тавсифлайди. Спецификациялар эса архитектура белгилаган ахборот тизи-

мини қандай қуриш лозимлигини ва ташкилий талабларни қандай қондирилишини аниқлайди.

Халқаро эътирофни қозонган ва ахборот хавфсизлиги сохасида кейинги ишланмаларда жуда кучли таъсир кўрсатган биринчи бахолаш стандарти АҚШ мудофаа вазирлигининг «*Тўқсариқ китоб*» (муқованинг ранги бўйича) деб аталувчи «Ишончли компьютер тизимларини бахолаш мезонлари» (Department of Defeuse Trusted Computer System Evaliation Criteria, TCSEC) стандарти бўлди. Муболағасиз тасдиқлаш мумкинки, «Тўқсариқ китоб»и ахборот хавфсизлигининг тушунчалар негизини ифодалайди. Ундаги тушунчаларнинг санаб ўтишнинг ўзи етарли: *хавфсиз ва ишончли тизимлар, хавфсизлик сиёсати, кафолатлик даражаси, хисоб-китоблилиги, ишончли ҳисоблаш асоси, мурожаатлар монитори, хавфсизликнинг ядроси ва периметри.*

«Тўқсарик китоб»дан сўнг чиқарилган хужжатлардан бири *«Тўқсарик китоб»нинг тармоқ конфигурациялари учун изохи»* (Trusted Network Interpretation) энг муҳим хужжат ҳисобланади. Бу хужжат икки кисмдан иборат. Биринчи қисм изохнинг ўзига бағишланган бўлса, иккинчи қисмида ўзига хос ёки тармоқ конфигурациялари учун айниқса муҳим бўлган *хавфсизлик сервислари* тавсифланади. Биринчи қисмга киритилган энг муҳим тушунчалардан бири – тармоқдаги ишончли ҳисоблаш асоси. Муҳим жиҳат–тармоқ конфигурацияларининг динамиклиги. Ҳимоялаш механизмлари орасида *конфиденциалликлик* ва *яхлитликни* таъминловчи *криптография* ажратилган. Фойдаланувчанлик масалалари, уни таъминлашдаги архитектуравий принципларнинг шакллантирилиши ўз вақти учун тартибли ёндашиши бўлди.

Тақсимланган ахборот тизимларини обьектга мўлжалланган тарзда коммуникацияларни криптографик ҳимоялаш билан биргаликда декомпозициялашнинг назарий асосини – мурожаатлар мониторини фрагментлашнинг корректлиги шартининг етарлилигини айтиб ўтиш лозим.

Баҳолаш стандартларидан яна бири *«Европа мамлакатларининг уйгунлаштирилган мезонлари»*да ахборот тизими ишлаши лозим бўлган шароитларга априор шартлар йўқ. Фараз қилинадики, аввал баҳолаш мақсади ифодаланади, сўнгра сертификациялаш органи бу мақсадга

қанчалик тўлиқ эришилишини, яъни, муайян вазиятда хавфсизликнинг архитектураси ва амалга оширилиши механизмларининг қанчалик корректлигини ва самаралилигини аниқлайди. Баҳолаш мақсадини ифодалашни енгиллаштириш ниятида стандартда хукумат ва тижорат тизимларига хос функционалликнинг ўнта тахминий синфлари тавсифланган.

Ушбу стандартда ахборот технологиялар тизимлари ва махсулотлари ўртасидаги фарқ таъкидланади, аммо талабларини унификациялаш ниятида ягона - *баҳолаш обьекти* тушунчаси киритилади. Стандартда хавфсизлик функциялари (сервислари) ва уларни амалга оширувчи механизмлар орасида фарқнинг кўрсатилиши ҳамда кафолатланишнинг икки жиҳати – хавфсизлик воситаларининг *самарадорлиги* ва *корректлигининг* ажратилиши муҳим ҳисобланади. Баҳолаш стандартлари гурухига ахборот хавфсизлигининг муайян, аммо мухим ва мураккаб жихатини регламентловчи АҚШнинг *«Криптографик модуллар учун хавфсизлик талаблари"* Федерал стандарти ҳамда *«Ахборот технологиялар хавфсизлигини бахоловчи мезонлар»* халқаро стандарти тааллуқли.

Техник спецификациялар орасида биринчи ўринга, сўзсиз, X800 «Очик тизимлар ўзаро ҳаракати учун хавфсизлик архитектураси» хужжатини қуйиш лозим. Бу хужжатда хавфсизликнинг энг мухим тармоқ сервислари ажратилган: *аутентификация*, *фойдаланишни бошқариш*, маълумотларни конфиденциаллиги ва ёки яхлитлигини таъминлаш, ҳамда қилинган ҳаракатдан *тонишнинг мумкин эмаслиги*. Сервисларни амалга ошириш учун хавфсизликнинг қуйидаги тармоқ механизмлари ва уларнинг комбинациялари кўзда тутилган: *шифрлаш, электрон рақамли имзо,* фойдаланишни бошқариш, маълумотлар яхлитлигининг назорати, аутентификация, *трафикни тўлдириш, маршрутлашни бошқариш, нотаризация*. Хавфсизликнинг сервислари ва механизмлари амалга оширилувчи етти сатҳли эталон моделининг сатҳлари танланган. Нихоят, тақсимланган конфигурациялар учун хавфсизлик воситаларининг маъмурлаш масалалари батафсил кўриб чикилган.

Internet – уюшманинг RFC 1510 «Аутентификациянинг тармоқ сервери Kerberos (VS)» спецификацияси хусусий, аммо мухим ва долзарб му-

аммога турли тақсимланган мухитда тармоққа ягона кириш концепциясини мададлаган ҳолда аутентификациялашга тегишли.

Kerberos аутентификациялаш сервери ишончли учинчи тараф бўлиб, хизмат курсатилувчи субьектларнинг махфий калитларига эга ва уларга ҳақиқийликнинг жуфтлашиб текширишда ёрдам беради. Kerberosнинг мижоз компонентларининг аксарият замонавий операцион тизимларда мавжудлиги унинг канчалик мухим эканлигидан далолат беради.

IPsec техник спецификацияси тармоқ сатҳида конфиденциаллик ва яхлитлик воситаларининг тўлиқ тўпламини тавсифланган ҳолда, муболағасиз фундаментал аҳамиятга эга. IPsec асосида юқорироқ сатҳ (татбиқий сатҳга қадар) протоколларини химоялаш механизми хамда хавфсизликнинг тугалланган воситалари, хусусан вертуал хусусий тармоқлар қурилади. Албатта IPsec криптографик механизмларига ва калит инфратузилмаларига таянади.

Транспорт сатҳи хавфсизлиги ва сигналлари (Transport Layer Security, TLS) хам шундай характерланади. TLS спецификацияси турли вазифаларни бажарувчи кўпгина дастурий махсулотларда ишлатилувчи оммавий Secure Socket Layer (SSL) протоколини ривожлантиради ва ойдинлаштиради.

Юқорида эслатиб ўтилган инфратузилма нуқтаи назаридан X.500 «*Директория хизмати*: концепциялар, моделлар ва серверлар обзори» (The Directory: Overview of consepts, models and services) ва X.509 «*Директория хизмати: сертификатлар, очиқ калитлар ва атрибутлар каркаслари*» (The Directory: Pubbic-key and attributc sertificate framworks) тавсиялари жуда муҳим ҳисобланади. X.509 тавсияларида очиқ калитлар ва атрибутлар яъни очиқ калитлар инфратузилмаси ва имтиёзларни бошқаришнинг базавий элементлари сертификатларининг формати тавсифланган.

Маълумки, ахборот хавфсизлигини таъминлаш компелкс муаммо бўлиб, қонуний, маъмурий, муолажавий ва дастурий-техник сатҳларда чораларни келишилган ҳолда кўришни талаб этади.

Маъмурий сатҳнинг базавий хужжати ташкилот *хавфсизлиги сиёсатини* ишлаб чиқишда ва амалга оширишда Internet - уюшманинг «Ташкилот ахборот хавфсизлиги бўйича қўлланма»си (Site Security Handbook)

наъмунали кўмакчи вазифасини ўташи мумкин. Унда хавфсизлик сиёсати муолажаларини шакллантирилишининг амалий жиҳатлари ёритилади, маъмурий ва муолажавий сатҳларнинг асосий тушунчалари изохланади, тавсия этувчи харакатларнинг сабаблари кўрсатилганган, хавф-хатарлар тахлили, ахборот хавфсизлигининг бузилишига муносабат ва бузилиш бартараф этилганидан кейинги харакат мавзуларига тўхтаб ўтилган.

«Ахборот химояси бузилишига қандай муносабат билдириш лозим» (Expections for Computer Security Incident Response) тавсиясида юқорида келтирилган масалалардан ташқари фойдали ахборот ресурсларига хаволаларни хамда муолажавий даражадаги амалий маслахатларни топиш мумкин.

Корпоратив ахборот тизимини ривожлантиришда ва қайта тузишда «*Internet-хизмат билан таъминловчини* қандай танлаш лозим» (Site Security Handbook Addendum for ISPs) тавсияси сўзсиз фойдалидир. Биринчи галда унинг қоидаларига ташкилий ва архитектуравий химоялашни шакллантириш жараёнида риоя қилиш лозим.

Британия стандарти BS 7799 «Ахборот хавфсизлигини бошқариш. Амалий қоидалар» (Code of practice for information security managment) ахборот хавфсизлигига жавобгар ташкилот рахбарлари учун фойдали ҳисобланади. Бу стандарт жиддий ўзгартиришсиз ISO/IEC 17799 халқаро стандартга кўчирилган.

Бу борада мустақил диёримиз Ўзбекистон Республикасида аҳамиятга молик бўлган улкан ишлар олиб борилмоқда. Бунга мисол тариқасида Ўзбекистон алоқа ва ахборотлаштириш агентлигининг илмий-техник ва маркетинг тадқиқотлари маркази томонидан ишлаб чиқилган O’z DSt 1092:2005 "Ахборот технологияси. Маълумотларни криптографик муҳофазаси. Электрон рақамли имзони шакллантириш ва текшириш жараёнлари", O’z DSt 1105:2006 "Ахборот технологияси. Маълумотларни криптографик муҳофазаси. Маълумотларни шифрлаш алгоритми", O’z DSt 1106:2006 "Ахборот технологияси. Маълумотларни криптографик муҳофазаси. Хешлаш функцияси" ва O’z DSt 1108:2006 "Ахборот технологияси. Очиқ тизимлар ўзаро боғлиқлиги. Электрон рақамли имзо очиқ калити сертификати ва атрибут сертификатининг тузилмаси" стандартларини

ва RH 45-187:2006 «Хавфсизлик талаблари» бошқарув хужжатини кўрсатиб ўтиш мумкин. Ушбу марказ томонидан ишлаб чиқилган стандартлар №05-11 12.04.2006 йилда Ўзбекистон стандартлаштириш, метрология ва сертификациялаш агентлиги томонидан тасдиқланган.

Бундан ташқари юртимизда ахборот хавфсизлиги соҳасида фаолият юритаётган Ўзбекистон алоқа ва ахборотлаштириш агентлиги қошидаги “Илмий-техник ва маркетинг тадқиқотлари маркази”, «UzInfocom» ва бошқа ташкилотларни айтиб ўтиш мақсадга мувофиқ. Чунки бу ташкилотларнинг юртимиз равнақи учун кўшаётган хиссаси катта аҳамиятга эга.

V боб. АХБОРОТНИ ҲИМОЯЛАШНИНГ КРИПТОГРАФИК УСУЛЛАРИ

5.1. Криптографиянинг асосий қоидалари ва таърифлари

Ахборотнинг ҳимоялашнинг аксарият механизмлари асосини шифрлаш ташкил этади. *Ахборотни шифрлаш* деганда очиқ ахборотни (дастлабки матнни) шифрланган ахборотга ўзгартириш (шифрлаш) ва аксинча (расшифровка қилиш) жараёни тушунилади. Шифрлаш криптотизимининг умумлаштирилган схемаси 5.1-расмда келтирилган.

5.1-расм. Шифрлаш криптотизимининг умумлаштирилган схемаси.

Узатилувчи ахборот матни M криптографик ўзгартириш E_{k1} ёрдамида шифрланади, натижада шифрматн C олинади:

$$C = E_{k1}(M)$$

бу ерда $k1$ – шифрлаш калити деб аталувчи E функциянинг параметри.

Шифрлаш калити ёрдамида шифрлаш натижаларини ўзгартириш мумкин. Шифрлаш калити муайян фойдаланувчига ёки фойдаланувчилар гуруҳига тегишли ва улар учун ягона бўлиши мумкин. Муайян калит ёрдамида шифрланган ахборот фақат ушбу калит эгаси (ёки эгалари) томонидан расшифровка қилиниши мумкин.

Ахборотни тескари ўзгартириш қуйидаги кўринишга эга:

$$M' = D_{k2}(C)$$

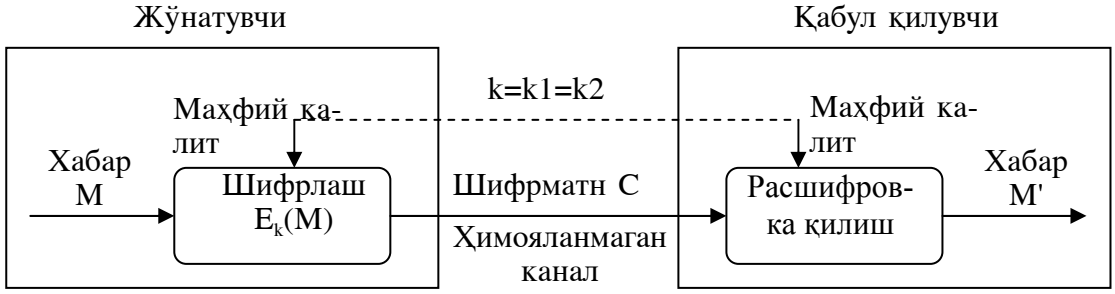
D функцияси E функцияга нисбатан тескари функция бўлиб, шифр матнни расшифровка қилади. Бу функция ҳам $k2$ калит кўринишидаги қўшимча параметрга эга. $k1$ ва $k2$ калитлар бир маъноли мосликка эга

бўлишлари шарт. Бу ҳолда расшифровка қилинган M' ахборот M га эквивалент бўлади. $k2$ калити ишончли бўлмаса D функция ёрдамида $M' = M$ дастлабки матнни олиб бўлмайди.

Криптотизимларнинг иккита синфи фарқланади:

- симметрик криптотизим (бир калитли);
- асимметрик криптотизим (иккита калитли).

Шифрлашнинг симметрик криптотизимида шифрлаш ва расшифровка қилиш учун битта калитнинг ўзи ишлатилади. Демак, шифрлаш калитидан фойдаланиш хуқуқига эга бўлган ҳар қандай одам ахборотни расшифровка қилиши мумкин. Шу сабабли, симметрик криптотизимлар маҳфий калитли криптотизимлар деб юритилади. Яъни шифрлаш калитидан фақат ахборот аталган одамгина фойдалана олиши мумкин. Шифрлашнинг симметрик криптотизими схемаси 5.2-расмда келтирилган.



5.2-расм. Симметрик шифрлаш криптотизимининг схемаси.

Электрон хужжатларни узатишнинг конфиденциаллигини симметрик криптотизим ёрдамида таъминлаш масаласи шифрлаш калити конфиденциаллигини таъминлашга келтирилади. Одатда, шифрлаш калити маълумотлар файли ва массивидан иборат бўлади ва шахсий калит элтувчисидан масалан, дискетда ёки смарт-картада сақланади. Шахсий калит элтувчиси эгасидан бошқа одамларнинг фойдаланишига қарши чоралар кўрилиши шарт.

Симметрик шифрлаш ахборотни "ўзи учун", масалан, эгаси йўқлигида ундан рухсатсиз фойдаланишни олдини олиш мақсадида, шифрлашда жуда қулай хисобланади. Бу танланган файлларни архивли шифрлаш ва бутун бир мантиқий ёки физик дискларни шаффоф(автоматик) шифрлаш бўлиши мумкин.

Симметрик шифрлашнинг ноқулайлиги - ахборот алмашинуви бошланмасдан олдин барча адресатлар билан махфий калитлар билан айирбошлаш заруриятидир. Симметрик криптотизимда махфий калитни алоқанинг умумфойдаланувчи каналлари орқали узатиш мумкин эмас. Махфий калит жўнатувчига ва қабул қилувчига калитлар тарқатилувчи ҳимояланган каналлар орқали узатилиши керак.

Симметрик шифрлаш алгоритмининг маълумотларни абонентли шифрлашда, яъни шифрланган ахборотни абонентга, масалан Internet орқали, узатишда амалга оширилган вариантлари мавжуд. Бундай криптографик тармоқнинг барча абонентлари учун бита калитнинг ишлатилиши хавфсизлик нуқтаи назаридан ножоиздир. Хақиқатан, калит обрўсизлантирилганда (йўқотилганида, ўғирлатилганда) барча абонентларнинг хужжат алмашиши хавф остида қолади. Бу ҳолда калитларнинг матрицаси (5.3-расм) ишлатилиши мумкин.

	1	2	3	…	n	
1	k_{11}	k_{12}	k_{13}	…	k_{1n}	1-абонент учун калитлар тўплами
2	k_{21}	k_{22}	k_{23}	…	k_{2n}	2- абонент учун калитлар тўплами
3	k_{31}	k_{32}	k_{33}	…	k_{3n}	3- абонент учун калитлар тўплами
…	…	…	…	…	…	…
n	k_{n1}	k_{n2}	k_{n3}	…	k_{nn}	n- абонент учун калитлар тўплами

5.3–расм. Калитлар матрицаси

Калитлар матрицаси абонентларнинг жуфт-жуфт боғланишли жадвалидан иборат. Жадвалнинг ҳар бир элементи *i* ва *j* абонентларни боғлашга мўлжалланган ва ундан фақат ушбу абонентлар фойдалана оладилар. Мос ҳолда, калитлар матрицаси элементлари учун қуйидаги тенглик ўринли.

$$K_{ij} = K_{ji}.$$

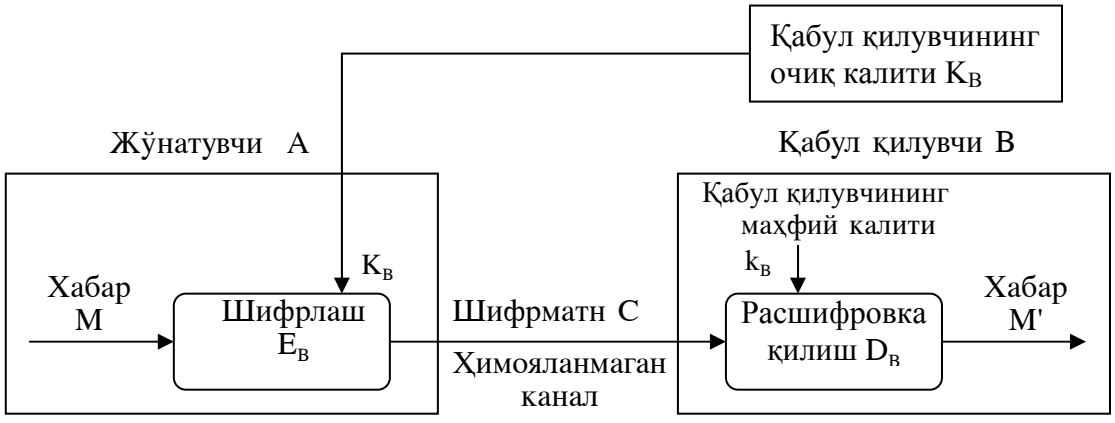
Матрицанинг ҳар бир *i*- қатори муайян *i* абонентнинг қолган *N*-1 абонентлар билан боғланишини таъминловчи калитлар тўпламидан иборат. Калитлар тўплами (тармоқ тўпламлари) криптографик тармоқнинг барча абонентлари ўртасида тақсимланади. Тақсимлаш алоқанинг *ҳимояланган каналлари* орқали ёки қўлдан-қўлга тарзда амалга оширилади.

Асимметрик криптотизимларда ахборотни шифрлашда ва расшифровка қилишда турли калитлардан фойдаланилади:

- *очиқ калит* K ахборотни шифрлашда ишлатилади, махфий калит k дан ҳисоблаб чиқарилади;
- *махфий калит* k, унинг жуфти бўлган очиқ калит ёрдамида шифрланган ахборотни расшифровка қилишда ишлатилади.

Махфий ва очиқ калитлар жуфт-жуфт генерацияланади. Махфий калит эгасида қолиши ва уни рухсатсиз фойдаланишдан ишончли химоялаш зарур (симметрик алгоритмдаги шифрлаш калитига ўхшаб). Очиқ калитнинг нусхалари махфий калит эгаси ахборот алмашинадиган криптографик тармоқ абонентларининг ҳар бирида бўлиши шарт.

Асимметрик шифрлашнинг умумлаштирилган схемаси 5.4-расмда келтирилган.



5.4-расм. Асимметрик шифрлашнинг умумлаштирилган схемаси.

Асимметрик криптотизимда шифрланган ахборотни узатиш қуйидагича амалга оширилади:

1. Тайёргарлик босқичи:

- абонент *B* жуфт калитни генерациялайди: махфий калит k_B ва очиқ калит K_B;

- очиқ калит K_B абонент A га ва қолган абонентларга жўнатилади.

2. A ва B абонентлар ўртасида ахборот алмашиш:

- абонент A абонент Bнинг очиқ калити K_B ёрдамида ахборотни шифрлайди ва шифрматнни абонент Bга жўнатади;

- абонент B ўзининг махфий калити k_B ёрдамида ахборотни расшифровка қилади. Ҳеч ким (шу жумладан абонент A ҳам) ушбу ахборотни расшифровка қилаолмайди, чунки абонент Bнинг маҳфий калити унда йўқ.

Асимметрик криптотизимда ахборотни химоялаш ахборот қабул қилувчи калити k_B нинг маҳфийлигига асосланган.

Асимметрик криптотизимларнинг асосий ҳусусиятлари қуйидагилар:

1. Очиқ калитни ва шифр матнни ҳимояланган канал орқали жўнатиш мумкин, яъни нияти бузуқ одамга улар маълум бўлиши мумкин.
2. Шифрлаш $E_B : M \rightarrow C$ ва расшифровка қилиш $D_B: C \rightarrow M$ алгоритмлари очиқ.

5.2. Симметрик шифрлаш тизими

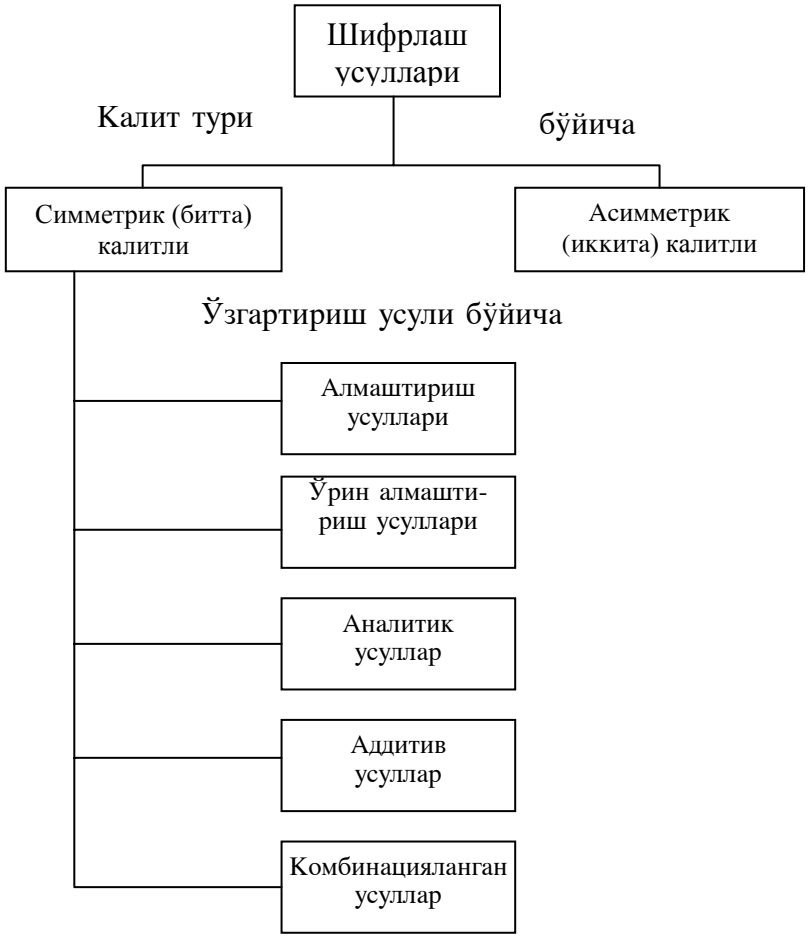
Шифрлаш усуллари турли аломатлари бўйича туркумланиши мумкин. Туркумланиш вариантларидан бири 5.5–расмда келтирилган.

Алмаштириш усуллари. Алмаштириш (подстановка) усулларининг моҳияти бир алфавитда ёзилган ахборот символларини бошқа алфавит символлари билан маълум қоида бўйича алмаштиришдан иборатдир. Энг содда усул сифатида ***тўғридан тўғри алмаштиришни*** кўрсатиш мумкин. Дастлабки ахборот ёзилувчи A_0 алфавитнинг s_{0i} символларига шифрловчи A_1 алфавитнинг s_{1i} символлари мос қуйилади. Оддий ҳолда иккала алфавит ҳам бир хил символлар тўпламига эга бўлиши мумкин.

Иккала алфавитдаги символлар ўртасидаги мослик маълум алгоритм бўйича К символлар узунлигига эга бўлган дастлабки матн T_0 символларининг рақамли эквивалентларини ўзгартириш орқали амалга оширилади.

Моноалфавитли алмаштириш алгоритми қуйидаги қадамлар кетма-кетлиги кўринишда ифодаланиши мумкин

1-қадам. [1xR] ўлчамли дастлабки A_0 алфавитдаги ҳар бир символ s_0 Є T(i=$\overline{1,K}$) ни A_0 алфавитдаги s_{0i} символ тартиб рақамига мос келувчи $h_{0i}(s_{0i})$ сонга алмаштириш йўли билан рақамлар кетма-кетлиги L_{0h} ни шакллантириш.



5.5-расм. Шифрлаш усулларининг туркумланиши.

2-қадам. L_{0h} кетма-кетлигининг ҳар бир сонини h_{1i}=(k_1x$h_{0i}(s_{0i})$+ k_2)(mod$R$) формула орқали ҳисобланувчи L_{1h} кетма-кетликнинг мос сони h_{1i} га алмаштириш йўли билан L_{1h} сон кетма-кетлигини шакллантириш, бу ерда k_1-ўнлик коэффицент; k_2-силжитиш коэффициенти. Танланган k_1, k_2 коэффицентлар h_{0i}, h_{1i} сонларнинг бир маъноли мослигини таъминлаши лозим, h_{1i}=0 олинганида эса h_{1i}=R алмашинуви бажарилиши керак.

3-қадам. L_{1h} кетма-кетликнинг ҳар бир сони $h_{1i}(s_{1i})$ни [1xR] ўлчамли шифрлаш алфавитнинг мос s_{1i} Є $T_1(i=\overline{1,K})$ символи билан алмаштириш йўли билан T_1 шифрматнни ҳосил қилиш.

4-қадам. Олинган шифрматн ўзгармас b узунликдаги блокларга ажратилади. Агар охирги блок тўлиқ бўлмаса блок орқасига махсус символ-тўлдирувчилар жойлаштирилади(масалан, *).

Мисол. Шифрлаш учун дастлабки маълумотлар қуйидагилар:

T_0=<ҲИМОЯ_ХИЗМАТИ>

A_0=<АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒҲ_>

A_1=<ОРЁЬЯТЭ-ЖМЧХАВДЙФҚКСЕЗПИЦГҲЛЪШБУЮ ҚГН>

R=36; k_1=3; k_2=15; b=4

Алгоритмнинг қадамба-қадам бажарилиши қуйидаги натижаларни олинишига олиб келади.

1-қадам. L_{oh}=<35,10,14,16,31,36,23,10,9,14,1,20,10>

2-қадам. L_{1h}=<12,9,21,17,36,14,12,9,6,21,18,3,9>

3-қадам. T_1=<ХЖЕФНВҲЖТЕҚЁЖ>

4-қадам. T_1=<ХЖЕФ НВҲЖ ТЕҚЁ Ж***>

Расшифровка қилишда блоклар бирлаштирилиб K символли шифрматн T_1 ҳосил қилинади. Расшифровка қилиш учун қуйидаги бутун сонли тенгламани ечиш лозим:

$$k_1 h_{01} + k_2 = nR + h_{1i}$$

k_1, k_2, h_{11} ва R бутун сонлар маълум бўлганда h_{0i} катталиги n ни саралаш орқали ҳисобланади. Бу муолажани шифрматннинг барча символларига тадбиқ қилиш унинг расшифровка қилинишига олиб келади.

Алмаштириш усулининг камчилиги сифатида дастлабки ва берилган матнлар статистик характеристкаларининг бир хиллигидир. Дастлабки матн қайси тилда ёзилганлигини билган криптоаналитик ушлаб қолинган ахборотларни статистик ишлаб, иккала алфавитдаги символлар ўртасидаги мувофиқликни аниқлаши мумкин.

Полиалфавитли алмаштириш усуллари айтарлича юқори криптобардошликка эга. Бу усуллар дастлабки матн символларини алмаштириш учун бир неча алфавитдан фойдаланишга асосланган. Расман полиалфавитли алмаштиришни қуйидагича тасаввур этиш мумкин. N-алфавитли алмаштиришда дастлабки A_0 алфавитдаги s_{01} символи A_1 алфавитдаги s_{11} символи

билан алмаштирилади ва ҳ. s_{0N} ни s_{NN} символ билан алмаштирилганидан сўнг $S_{0(N+1)}$ символнинг ўрнини A_1 алфавитдаги $S_{1(N+1)}$ символ олади ва ҳ.

Полиалфавитли алмаштириш алгоритмлари ичида ***Вижинер жадвали (матрицаси)*** T_B ни ишлатувчи алгоритм энг кенг тарқалган. Вижинер жадвали [*R*x*R*] ўлчамли квадрат матрицадан иборат бўлиб, (*R*-ишлатилаётган алфавитдаги символлар сони) биринчи қаторида символлар алфавит тартибида жойлаштирилади. Иккинчи қатордан бошлаб символлар чапга битта ўринга силжитилган ҳолда ёзилади. Сиқиб чиқарилган символлар ўнг тарафдаги бўшаган ўринни тўлдиради (циклик силжитиш). Агар ўзбек алфавити ишлатилса, Вижинер матрицаси [36x36] ўлчамга эга бўлади (5.5-расм).

АБВГД.....	.....	.....ЎҚҒҲ_
БВГДЕ.....	.....	.....ҚҒҲ_А
ВГДЕЖ.....	.....	.....ҒҲ_АБ
.....		
_АБВГ.....	.....	.....ЯЎҚҒҲ

5.6-расм. Вижинер матрицаси.

Шифрлаш такрорланмайдиган *M* символдан иборат калит ёрдамида амалга оширилади. Вижинернинг тўлиқ матрицасидан [*(M+1),R*] ўлчамли шифрлаш матрицаси $T_{(Ш)}$ ажратилади. Бу матрица биринчи қатордан ва биринчи элементлари калит символларига мос келувчи қаторлардан иборат бўлади.

Агар калит сифатида <ҒЎЗА> сўзи танланган бўлса, шифрлаш матрицаси бешта қатордан иборат бўлади. (5.7-расм)

$T_ш$

АБВДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒҲ_
ҒҲ_АБВДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚ
ЎҚҒҲ_АБВДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯ
ЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒҲ_АБВДЕЁЖ
АБВДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒҲ_

5.7-расм. «Ғўза» калити учун шифрлаш матрицаси.

Вижинер жадвали ёрдамида шифрлаш алгоритми қуйидаги қадамлар кетма-кетлигидан иборат.

1-қадам. Узунлиги M символли калит K ни танлаш.

2-қадам. Танланган калит K учун $[(M+1),R]$ ўлчамли шифрлаш матрицаси $T_ш=(b_{ij})$ ни қуриш.

3- қадам. Дастлабки матннинг ҳар бир символи s_{0r} тагига калит символи k_m жойлаштирилади. Калит кераклича такрорланади.

4-қадам. Дастлабки матн символлари шифрлаш матрицаси $T_ш$ дан қуйидаги қоида бўйича танланган символлар билан кетма-кет алмаштирилади.

1) K калитнинг алмаштирилувчи s_{0r} символга мос k_m символи аниқланади;

2) шифрлаш матрицаси $T_ш$ даги $k_m = b_{j1}$ шарт бажарилувчи i қатор топилади.

3) $s_{or} = b_{i1}$ шарт бажарилувчи j устун аниқланади.

4) s_{or} символи b_{ij} символи билан алмаштирилади.

5-қадам. Шифрланган кетма-кетлик маълум узунликдаги (масалан 4 символли) блокларга ажратилади. Охирги блокнинг бўш жойлари махсус символ-тўлдирувчилар билан тўлдирилади.

Расшифровка қилиш қуйидаги кетма-кетликда амалга оширилади.

1-қадам. Шифрлаш алгоритмининг 3-қадамидагидек шифрматн тагига калит символлари кетма-кетлиги ёзилади.

2-қадам. Шифрматндан s_{1r} символлари ва мос калит символлари k_m кетма-кет танланади. $T_ш$ матрицада $k_m = b_{ij}$ шартни қаноатлантирувчи i қатор аниқланади. i-қаторда $b_{ij}=s_{1r}$ элемент аниқланади. Расшифровка қилинган матнда r - ўрнига b_{ij} символи жойлаштирилади.

3-қадам. Расшифровка қилинган матн ажратилмасдан ёзилади. Хизматчи символлар олиб ташланади.

Мисол. K=<FЎЗA> калити ёрдамида T=<ПАХТА FАРАМИ> дастлабки матнни шифрлаш ва расшифровка қилиш талаб этилсин. Шифрлаш ва расшифровка қилиш механизми 5.7-расмда келтирилган

Полиалфавитли алмаштириш усулларининг криптобардошлиги оддий алмаштириш усулларига қараганда айтарлича юқори, чунки уларда дастлабки кетма-кетликнинг бир хил символлари турли символлар билан алмаштирилиши мумкин. Аммо шифрнинг статистик усулларига бардошлилиги калит узунлигига боғлиқ.

Дастлабки матн	ПАХТА_ҒАРАМИ
Калит	Ғ ЎЗАҒЎЗАҒЎЗ А
Алмаштирилган сўнгги матн	МЎЯТҒЯЕАНЎФИ
Шифрматн	МЎЯТ ҒЯЕА НЎФИ
Калит	ҒЎЗА ҒЎЗА ҒЎЗА
Расшифровка қилинган матн	ПАХТ А_ҒА РАМИ
Дастлабки матн	ПАХТА_ҒАРАМИ

5.8-расм. Вижинер матрицаси ёрдамида шифрлаш мисоли.

Ўрин алмаштириш усуллари. Ўрин алмаштириш усулларига биноан дастлабки матн белгиланган узунликдаги блокларга ажратилиб ҳар бир блок ичидаги символлар ўрни маълум алгоритм бўйича алмаштирилади.

Энг осон ўрин алмаштиришга мисол тариқасида дастлабки ахборот блокини матрицага қатор бўйича ёзишни, ўқишни эса устун бўйича амалга оширишни кўрсатиш мумкин. Матрица қаторларини тўлдириш ва шифрланган ахборотни устун бўйича ўқиш кетма-кетлиги калит ёрдамида берилиши мумкин. Усулнинг криптобардошлиги блок узунлигига (матрица ўлчамига) боҒлиқ. Масалан узунлиги 64 символга тенг бўлган блок (матрица ўлчами 8х8) учун калитнинг $1{,}6 \bullet 10^9$ комбинацияси бўлиши мумкин. Узунлиги 256 символга тенг бўлган блок (матрица ўлчами 16х16) калитнинг мумкин бўлган комбинацияси $1{,}4 \bullet 10^{26}$ га етиши мумкин. Бу ҳолда калитни саралаш масаласи замонавий ЭҲМлар учун ҳам мураккаб ҳисобланади.

Гамильтон маршрутларига асосланган усулда ҳам ўрин алмаштиришлардан фойдаланилади. Ушбу усул қуйидаги қадамларни бажариш орқали амалга оширилади.

1-қадам. Дастлабки ахборот блокларга ажратилади. Агар шифрланувчи ахборот узунлиги блок узунлигига каррали бўлмаса, охирги блокдаги

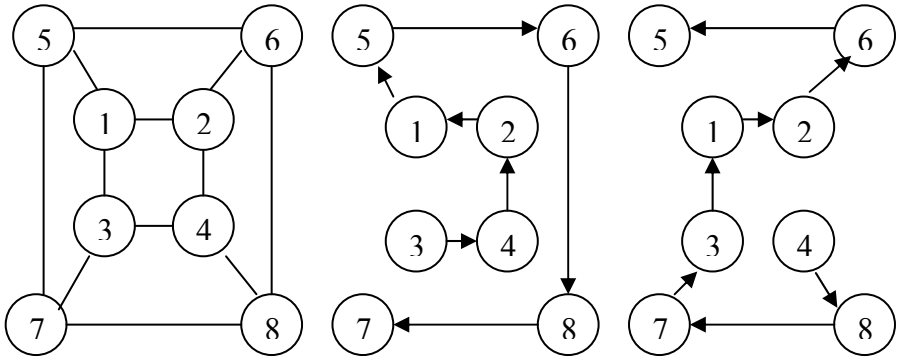
бўш ўринларга махсус хизматчи символлар-тўлдирувчилар жойлаштирилади(масалан, *).

2-қадам. Блок символлари ёрдамида жадвал тўлдирилади ва бу жадвалда символнинг тартиб рақами учун маълум жой ажратилади (5.9-расм).

3-қадам. Жадвалдаги символларни ўқиш маршрутларнинг бири бўйича амалга оширилади. Маршрутлар сонининг ошиши шифр криптобардошлигини оширади. Маршрутлар кетма-кет танланади ёки уларнинг навбатланиши калит ёрдамида берилади.

4-қадам. Символларнинг шифрланган кетма-кетлиги белгиланган *L* узунликдаги блокларга ажратилади. *L* катталик 1-қадамда дастлабки ахборот бўлинадиган блоклар узунлигидан фарқланиши мумкин.

Расшифровка қилиш тескари тартибда амалга оширилади. Калитга мос ҳолда маршрут танланади ва бу маршрутга биноан жадвал тўлдирилади.



5.9-расм. 8-элементли жадвал ва Гамильтон маршрутлари вариантлари.

Жадвалдан символлар элемент номерлари келиши тартибида ўқилади.

Мисол. Дастлабки матн T_0 «ЎРИН АЛМАШТИРИШ УСУЛИ»ни шифрлаш талаб этилсин. Калит ва шифрланган блоклар узунлиги мос ҳолда қуйидагиларга тенг: *K*=<2,1,1>, *L*=4. Шифрлаш учун 5.9-расмда келтирилган жадвал ва иккита маршрутдан фойдаланилади. Берилган шартлар учун матрицалари тўлдирилган маршрутлар 5.10-расмда келтирилган кўринишга эга.

1-қадам. Дастлабки матн учта блокка ажратилади. *Б1*=<ЎРИН_АЛМ>, *Б2*=<АШТИРИШ->, *Б3*=<УСУЛИ**>;

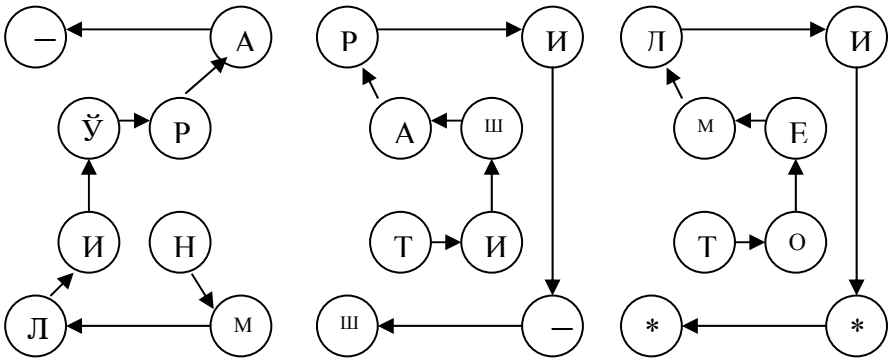
2-қадам. 2,1,1 маршрутли учта матрица тўлдирилади;

3-қадам. Маршрутларга биноан символларни жой-жойига қўйиш орқали шифрматнни ҳосил қилиш.

T_1=<НМЛИЎРА_ТИШАРИ_ШТОЕМДИ**>

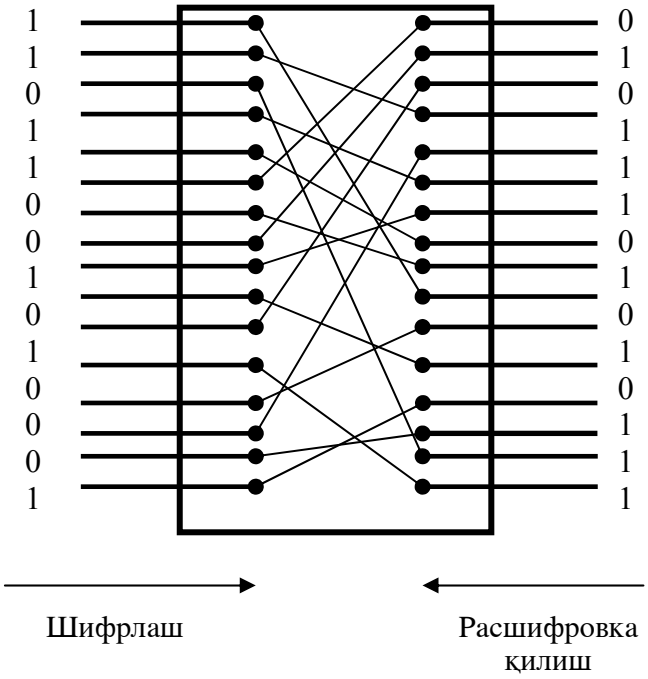
4-қадам. Шифрматнни блокларга ажратиш.

T_1=<НМЛИ ЎРА_ ТИША РИ_Ш ТОЕМ ДИ**>



5.10-расм. Гамильтон маршрути ёрдамида шифрлаш мисоли.

Амалиётда ўрин алмаштириш усулини амалга оширувчи махсус аппарат воситалар катта аҳамиятга эга (5.11-расм).



5.11-расм. Ўрин алмаштириш схемаси.

Дастлабки ахборот блокининг параллел иккили коди (масалан, икки байт) схемага берилади. Ички коммутация ҳисобига схемада битларнинг

блоклардаги ўринлари алмаштирилади. Расшифровка қилиш учун эса сҳеманинг кириш ва чиқиш йўллари ўзаро алмаштирилади.

Ўрин алмаштириш усулларининг амалга оширилиши содда бўлсада, улар иккита жиддий камчиликларга эга. Биринчидан, бу усулларни статистик ишлаш орқали фош қилиш мумкин. Иккинчидан, агар дастлабки матн узунлиги *K* символлардан ташкил топган блокларга ажратилса, шифрни фош этиш учун шифрлаш тизимсига биттасидан бошқа барча символлари бир хил бўлган тест ахборотининг *K-1* блокини юбориш кифоя.

Шифрлашнинг аналитик усуллари. Матрица алгебрасига асосланган шифрлаш усуллари энг кўп тарқалган. Дастлабки ахборотнинг $B_к=||b_j||$ вектор кўринишида берилган *k*- блокини шифрлаш $A=||a_{ij}||$ матрица калитни $B_к$ векторга кўпайтириш орқали амалга оширилади. Натижада $C_k=||c_i||$ вектор кўринишидаги шифрматн блоки ҳосил қилинади. Бу векторнинг элементлари $c_i = \sum_j a_{ij} b_j$ ифодаси орқали аниқланади.

Ахборотни расшифровка қилиш C_k векторларини *A* матрицага тескари бўлган A^{-1} матрицага кетма-кет кўпайтириш орқали аниқланади.

Мисол. T_0=<АЙЛАНА> сўзини матрица-калит

$$A = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix}$$

ёрдамида шифрлаш ва расшифровка қилиш талаб этилсин.

Дастлабки сўзни шифрлаш учун қуйидаги қадамларни бажариш лозим.

1-қадам. Дастлабки сўзнинг алфавитдаги харфлар тартиб рақами кетма-кетлигига мос сон эквивалентини аниқлаш.

$$T_э = <1,10,12,1,14,1>$$

2-қадам. *A* матрицани $B_1=\{1,10,12\}$ ва $B_2=\{1,14,1\}$ векторларга кўпайтириш.

$$C_1 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 10 \\ 12 \end{vmatrix} = \begin{vmatrix} 137 \\ 97 \\ 156 \end{vmatrix}$$

$$C_2 = \begin{vmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{vmatrix} \cdot \begin{vmatrix} 1 \\ 14 \\ 1 \end{vmatrix} = \begin{vmatrix} 65 \\ 103 \\ 137 \end{vmatrix}$$

3-қадам. Шифрланган сўзни кетма-кет сонлар кўринишида ёзиш.

$$T_1 = <137,97,156,65,103,137>$$

Шифрланган сўзни расшифровка қилиш қуйидагича амалга оширилади:

1-қадам. A матрицанинг аниқловчиси ҳисобланади:

$$|A| = -115 .$$

2-қадам. Ҳар бир элементи А матрицадаги a_{ij} элементнинг алгебраик тўлдирувчиси бўлган бириктирилган матрица A^* аниқланади.

$$A^* = \begin{vmatrix} 17 & -3 & -15 \\ 52 & -43 & 15 \\ -48 & 22 & -5 \end{vmatrix}$$

3-қадам. Транспонирланган матрица A^T аниқланади.

$$A^T = \begin{vmatrix} 17 & 52 & -48 \\ -3 & -43 & 22 \\ -15 & 15 & -5 \end{vmatrix}$$

4-қадам. Қуйидаги формула бўйича тескари матрица A^{-1} ҳисобланади:

$$A^{-1} = \frac{A^t}{|A|}$$

Ҳисоблаш натижасида қуйидагини оламиз.

$$A^{-1} = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix}$$

5-қадам. B_1 ва B_2 векторлар аниқланади:

$$B_1 = A^{-1}C_1; \qquad B_2 = A^{-1}C_2 .$$

$$B_1 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 137 \\ 97 \\ 156 \end{vmatrix} = \begin{vmatrix} 1 \\ 10 \\ 12 \end{vmatrix}$$

$$B_2 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 65 \\ 103 \\ 137 \end{vmatrix} = \begin{vmatrix} 1 \\ 14 \\ 1 \end{vmatrix}$$

6-қадам. Расшифровка қилинган сўзнинг сон эквиваленти $T_э$=<1,10,12,1,14,1> символлар билан алмаштирилади. Натижада дастлабки сўз T_0=<АЙЛАНА> ҳосил бўлади.

Шифрлашнинг аддитив усуллари. Шифрлашнинг ***аддитив усулларига*** биноан дастлабки ахборот символларига мос келувчи рақам кодларини кетма-кетлиги ***гамма*** деб аталувчи қандайдир символлар кетма-кетлигига мос келувчи кодлар кетма-кетлиги билан кетма-кет жамланади. Шу сабабли, шифрлашиннг аддитив усуллари ***гаммалаш*** деб ҳам аталади.

Ушбу усуллар учун калит сифатида гамма ишлатилади. Аддитив усулнинг криптобардошлиги калит узунлигига ва унинг статистик характеристикаларининг текислигига боғлиқ. Агар калит шифрланувчи символлар кетма-кетлигидан қисқа бўлса, шифрматн криптоаналитик томонидан статистик усуллар ёрдамида расшифровка қилиниши мумкин. Калит ва дастлабки ахборот узунликлари қанчалик фарқланса, шифр-матнга муваффақиятли хужум эҳтимоллиги шунчалик ортади. Агар калит узунлиги шифрланувчи ахборот узунлигидан катта бўлган тасодифий сонларнинг даврий бўлмаган кетма-кетлигидан иборат бўлса, калитни билмасдан туриб шифрматнни расшифровка қилиш амалий жиҳатдан мумкин эмас. Алмаштириш усулларидагидек гаммалашда калит сифатида рақамларнинг такрорланмайдиган кетма-кетлиги ишлатилиши мумкин.

Амалиётда асосини псевдотасодифий сонлар генераторлари (датчиклари) ташкил этган аддитив усуллар энг кўп тарқалган ва самарали ҳисобланади. Генератор псевдотасодифий сонларнинг чексиз кетма-кетлигини шакллантиришда нисбатан қисқа узунликдаги дастлабки ахборотдан фойдаланади.

Псевдотасодифий сонлар кетма-кетлигини шакллантиришда конгруэнт генераторлардан ҳам фойдаланилади. Бу синф генераторлари сонларнинг шундай псевдотасодифий кетма-кетликларини шакллантирадики, улар учун генераторларнинг даврийлиги ва чиқиш йўли кетма-кетликларининг тасо-

дифийлиги каби асосий характеристкаларини қатъий математик тарзда ифодалаш мумкин.

Конгруэнт генераторлар ичида ўзининг соддалиги ва самаралилиги билан чизиқли генератор ажралиб тўради. Бу генератор қуйидаги муносабат бўйича сонларнинг псевдотасодифий кетма-кетликларини шакллантиради.

$$T(i+1) = (a \cdot T(i) + c) \bmod m;$$

бу ерда a ва c – ўзгармаслар, T(0) –туғдирувчи(сабаб бўлувчи) сон сифатида танланган дастлабки катталик.

Бундай датчикнинг такрорланиш даври a ва c катталикларига боғлиқ. m қиймати одатда 2^S га тенг қилиб олинади, бу ерда *s*-ЭХМдаги сўзнинг битлардаги узунлиги. Шакллантирувчи сон кетма-кетликларининг такрорланиш даври *c*-тоқ сон ва a (mod4)=1 бўлгандагина максималь бўлади. Бундай генераторларни аппарат ёки программ воситалари орқали осонгина яратиш мумкин.

Шифрлашнинг комбинацияланган усуллари. Қудратли компьютерлар, тармоқ технологиялари ва нейронли ҳисоблашларнинг пайдо бўлиши ҳозиргача умуман фош қилинмайди деб ҳисобланган криптографик тизимларни обрўсизлантирилишига сабаб бўлди. Бу эса ўз навбатида юқори бардошликка эга криптографик тизимларни яратиш устида ишлашни тақозо этди. Бундай криптографик тизимларни яратиш усулларидан бири шифрлаш усулларини комбинациялашдир. Қуйида энг кам вақт сарфида криптобардошликни жиддий ошишини таъминловчи шифрлашнинг комбинацияланган усули устида сўз боради. Шифрлашнинг ушбу комбинацияланган усулига биноан маълумотларни шифрлаш икки босқичда амалга оширилади. Биринчи босқичда маълумотлар стандарт усул (масалан, DES усул) ёрдамида шифрланса, иккинчи босқичда шифрланган маълумотлар махсус усул бўйича қайта шифрланади. Махсус усул сифатида маълумотлар векторини элементлари нолдан фарқли бўлган сон матрицасига кўпайтиришдан фойдаланиш мумкин.

Гаммалашни қўллашда агар шифр гаммаси сифатида рақамларнинг такрорланмайдиган кетма-кетлиги ишлатилса шифрланган матнни фош қилиш жуда қийин. Одатда шифр гаммаси ҳар бир шифрланувчи сўз учун

тасодифий ўзгариши лозим. Агар шифр гаммаси шифрланган сўз узунлигидан катта бўлса ва дастлабки матннинг ҳеч қандай қисми маълум бўлмаса, шифрни фақат тўғридан-тўғри саралаш орқали фош этиш мумкин. Бунда криптобардошлик калит ўлчами орқали аниқланади. Шифрлашнинг бу усулидан кўпинча ҳимоя тизимининг дастурий амалга оширилишида фойдаланилади ва шифрлашнинг бу усулига асосланган тизимларда бир секундда маълумотларнинг бир неча юз Кбайтини шифрлаш имконияти мавжуд. Расшифровка қилиш жараёни-калит маълум бўлганида шифр гаммасини қайта генерациялаш ва уни шифрланган маълумотларга сингдиришдан иборат.

Шифрланган маълумотлар векторини матрицага кўпайтиришни қўллашда шифрланган матн бир байт узунликдаги f_i векторларга ажратилади ва ҳар бир вектор квадрат матрица $\left\| M_{ij} \right\|$ га кўпайтирилади ва шифрланган векторлар шакллантирилади:

$$f_i^* = f_i \cdot \left\| M_{ij} \right\|$$

Бу усулнинг асосий афзаллиги сифатида унинг маълумотлар ишланишининг турли жабхаларидаги мосланувчанлигини кўрсатиш мумкин. Ҳар бир вектор алоҳида шифрланганлиги сабабли маълумотлар блокини узатиш ва дастурланган маълумотлардан ихтиёрий фойдаланиш имконияти туғилади. Ушбу усулни аппарат ёки дастурий усулда амалга ошириш мумкин.

Расшифровка қилиш жараёнида шифрланган f^* векторларни тескари матрица $\left(\left\| M_{ij}^{-1} \right\|\right)$га кўпайтирилади.

$$f_i = f_i^* \cdot \left\| M_{ij}^{-1} \right\|$$

Комбинацияланган усулларнинг юқори самарадорлигига унинг иккала босқичини аппарат усулда амалга ошириш орқали эришиш мумкин. Аммо бу ускуна харажатларининг жиддий ошишига олиб келади. Дастурий усулда амалга оширилишида эса маълумотларни шифрлаш ва расшифровка қилиш вақти ошиб кетади. Шу сабабли комбинацияланган усуларни аппарат-дастурий усулда, яъни усулнинг бир босқичи аппарат усулда, иккинчи

босқичи дастурий усулда амалга оширилиши мақсадга мувофиқ ҳисобланади.

5.3. Асимметрик шифрлаш тизимлари

Асимметрик шифрлаш тизимларида иккита калит ишлатилади. Ахборот очиқ калит ёрдамида шифрланса, махфий калит ёрдамида расшифровка қилинади. Асимметрик шифрлаш тизимларини очиқ калитли шифрлаш тизимлар деб ҳам юритилади.

Очиқ калитли тизимларини қўллаш асосида қайтарилмас ёки бир томонли функциялардан фойдаланиш ётади. Бундай функциялар қуйидаги хусусиятларга эга. Маълумки x маълум бўлса $y=f(x)$ функцияни аниқлаш осон. Аммо унинг маълум қиймати бўйича x ни аниқлаш амалий жихатдан мумкин эмас. Криптографияда яширин деб аталувчи йўлга эга бўлган бир томонли функциялар ишлатилади. z параметрли бундай функциялар қуйидаги хусусиятларга эга. Маълум z учун E_z ва D_z алгоритмларини аниқлаш мумкин. E_z алгоритми ёрдамида аниқлик соҳасидаги барча x учун $f_Z(x)$ функцияни осонгина олиш мумкин. Худди шу тариқа D_z алгоритми ёрдамида жоиз қийматлар соҳасидаги барча y учун тескари функция $x=f^{-1}(y)$ ҳам осонгина аниқланади. Айни вақтда жоиз қийматлар соҳасидаги барча z ва деярли барча, y учун хатто E_z маълум бўлганида ҳам $f^{-1}(y)$ни ҳисоблашлар ёрдамида топиб бўлмайди. Очиқ калит сифатида y ишлатилса, махфий калит сифатида x ишлатилади.

Очиқ калитни ишлатиб шифрлаш амалга оширилганда ўзаро мулоқатда бўлган субъектлар ўртасида махфий калитни алмашиш зарурияти йўқолади. Бу эса ўз навбатида узатилувчи ахборотнинг криптоҳимоясини соддалаштиради.

Очиқ калитли криптотизимларни бир томонли функциялар кўриниши бўйича фарқлаш мумкин. Буларнинг ичида RSA, Эль-Гамал ва Мак-Элис тизимларини алохида тилга олиш ўринли. Ҳозирда энг самарали ва кенг тарқалган очиқ калитли шифрлаш алгоритми сифатида RSA алгоритмини

кўрсатиш мумкин. RSA номи алгоритмни яратувчилари фамилияларининг биринчи харфидан олинган (Rivest, Shamir ва Adleman).

Алгоритм модуль арифметикасининг даражага кўтариш амалидан фойдаланишга асосланган. Алгоритмни қуйидаги қадамлар кетма-кетлиги кўринишида ифодалаш мумкин.

1-қадам. Иккита 200дан катта бўлган туб сон p ва q танланади.

2-қадам. Калитнинг очиқ ташкил этувчиси n ҳосил қилинади

$$n=p*q.$$

3-қадам. Қуйидаги формула бўйича Эйлер функцияси ҳисобланади:

$$f(p,q)=(p-1)(q-1).$$

Эйлер функцияси n билан ўзаро туб, 1 дан n гача бўлган бутун мусбат сонлар сонини кўрсатади. Ўзаро туб сонлар деганда 1 дан бошқа бирорта умумий бўлувчисига эга бўлмаган сонлар тушунилади.

4-қадам. $f(p,q)$ қиймати билан ўзаро туб бўлган катта туб сон d танлаб олинади.

5-қадам. Қуйидаги шартни қаноатлантирувчи e сони аниқланади

$$e \cdot d = 1(mod f(p,q)).$$

Бу шартга биноан $e \cdot d$ кўпайтманинг $f(p,q)$ функцияга бўлишдан қолган қолдиқ 1га тенг. e сони очиқ калитнинг иккинчи ташкил этувчиси сифатида қабул қилинади. Махфий калит сифатида d ва n сонлари ишлатилади.

6-қадам. Дастлабки ахборот унинг физик табиатидан қатъий назар рақамли иккили кўринишда ифодаланади. Битлар кетма-кетлиги L бит узунликдаги блокларга ажратилади, бу ерда $L–L \geq \log_2(n+1)$ шартини қаноатлантирувчи энг кичик бутун сон. Ҳар бир блок [0, n-1] оралиқка тааллуқли бутун мусбат сон каби кўрилади. Шундай қилиб, дастлабки ахборот $X(i)$, $i=\overline{1,I}$ сонларнинг кетма-кетлиги орқали ифодаланади. i нинг қиймати шифрланувчи кетма-кетликнинг узунлиги орқали аниқланади.

7-қадам. Шифрланган ахборот қуйидаги формула бўйича аниқланувчи $Y(i)$ сонларнинг кетма-кетлиги кўринишида олинади:

$$Y(i) = (X(i))^e (\mathrm{mod}\, n).$$

Ахборотни расшифровка қилишда қуйидаги муносабатдан фойдаланилади:

$$X(i) = (Y(i))^d \,(\mathrm{mod}\, n).$$

Мисол. <ГАЗ> сўзини шифрлаш ва расшифровка қилиш талаб этилсин. Дастлабки сўзни шифрлаш учун қуйидаги қадамларни бажариш лозим.

1-қадам. p=3 ва q=11 танлаб олинади.

2-қадам. $n = 3 \cdot 11 = 33$ ҳисобланади.

3-қадам. Эйлер функцияси аниқланади.

$$f(p,q) = (3-1)\cdot(11-1) = 20$$

4-қадам. Ўзаро туб сон сифатида d=3 сони танлаб олинади.

5-қадам. $(e \cdot 3)\cdot(\mathrm{mod}\, 20) = 1$ шартини қаноатлантирувчи е сони танланади. Айтайлик, e=7.

6-қадам. Дастлабки сўзнинг алфавитдаги харфлар тартиб рақами кетма-кетлигига мос сон эквиваленти аниқланади. А харфига –1, Г харфига-4, З харфига –9. Ўзбек алфавитида 36та харф ишлатилиши сабабли иккили кодда ифодалаш учун 6 та иккили хона керак бўлади. Дастлабки ахборот иккили кодда қуйидаги кўринишга эга бўлади:

000100 000001 001001.

Блок узунлиги L бутун сонлар ичидан $L \ge \log_2(33+1)$ шартини қаноатлантирувчи минималь сон сифатида аниқланади. n=33 бўлганлиги сабабли L=6.

Демак, дастлабки матн $X(i) \le\!< 4,1,9 >$ кетма-кетлик кўринишида ифодаланади.

7-қадам. $X(i)$ кетма-кетлиги очиқ калит {7,33} ёрдамида шифрланади:

$$Y(1) = (4^7)(\mathrm{mod}\, 33) = 16384(\mathrm{mod}\, 33) = 16$$

$$Y(2) = (1^7)(\mathrm{mod}\, 33) = 1(\mathrm{mod}\, 33) = 1$$

$$Y(1) = (9^7)(\mathrm{mod}\, 33) = 4782969(\mathrm{mod}\, 33) = 15$$

Шифрланган сўз $Y(i)$=<16,1,15>

Шифрланган сўзни расшифровка қилиш махфий калит {3,33} ёрдамида бажарилади.:

$$Y(1) = (16^3)(\mathrm{mod}\,33) = 4096(\mathrm{mod}\,33) = 4$$

$$Y(1) = (1^3)(\mathrm{mod}\,33) = 1(\mathrm{mod}\,33) = 1$$

$$Y(1) = (15^3)(\mathrm{mod}\,33) = 3375(\mathrm{mod}\,33) = 9$$

Дастлабки сон кетма-кетлиги расшифровка қилинган $X(i)$=<4,1,9> кўринишида дастлабки матн <ГАЗ> билан алмаштирилади.

Келтирилган мисолда ҳисоблашларнинг соддалигини таъминлаш мақсадида мумкин бўлган кичик сонлардан фойдаланилди.

Эль-Гамал тизими чекли майдонларда дискрет логарифмларнинг ҳисобланиш мураккаблигига асосланган. RSA ва Эль-Гамал тизимларининг асосий камчилиги сифатида модуль арифметикасидаги мураккаб амалларнинг бажарилиши заруриятини кўрсатиш мумкин. Бу ўз навбатида айтарлича ҳисоблаш ресурсларини талаб қилади.

Мак-Элис криптотизимида хатоликларни тузатувчи кодлар ишлатилади. Бу тизим RSA тизимига нисбатан тезроқ амалга оширилсада, жиддий камчиликка эга. Мак-Элис криптотизимсида катта узунликдаги калит ишлатилади ва олинган шифрматн узунлиги дастлабки матн узунлигидан икки марта катта бўлади.

Барча очиқ калитли шифрлаш усуллари учун *NP*-тўлиқ масалани (тўлиқ саралаш масаласи) ечишга асосланган криптотахлил усулидан бошқа усулларининг йўқлиги қатъий исботланмаган. Агар бундай масалаларни ечувчи самарали усуллар пайдо бўлса, бундай хилдаги криптотизим обрўсизлантирилади.

Юқорида кўрилган шифрлаш усулларининг криптобардошлиги калит узунлигига боғлиқ бўлиб, бу узунлик замонавий тизимлар учун, лоақал, 90 битдан катта бўлиши шарт.

Айрим муҳим қўлланишларда нафақат калит, балки шифрлаш алгоритми ҳам маҳфий бўлади. Шифрларнинг криптобардошлигини ошириш учун бир неча калит (одатда учта) ишлатилиши мумкин. Биринчи калит ёрдамида шифрланган ахборот иккинчи калит ёрдамида шифрланади ва ҳ.

5.4. Шифрлаш стандартлари

Россиянинг ахборотни шифрлаш стандарти. Росссия Федерациясида ҳисоблаш машиналари, комплекслари ва тармоқларида ахборотни криптографик ўзгартириш алгоритмларига давлат стандарти (ГОСТ 2814-89) жорий этилган. Бу алгоритмлар махфийлик даражаси ихтиёрий бўлган ахборотни ҳеч қандай чекловсиз шифрлаш имконини беради. Алгоритмлар аппарат ва дастурий усулларида амалга оширилиши мумкин.

Стандартда ахборотни криптографик ўзгартиришнинг қуйидаги алгоритмлари мавжуд:

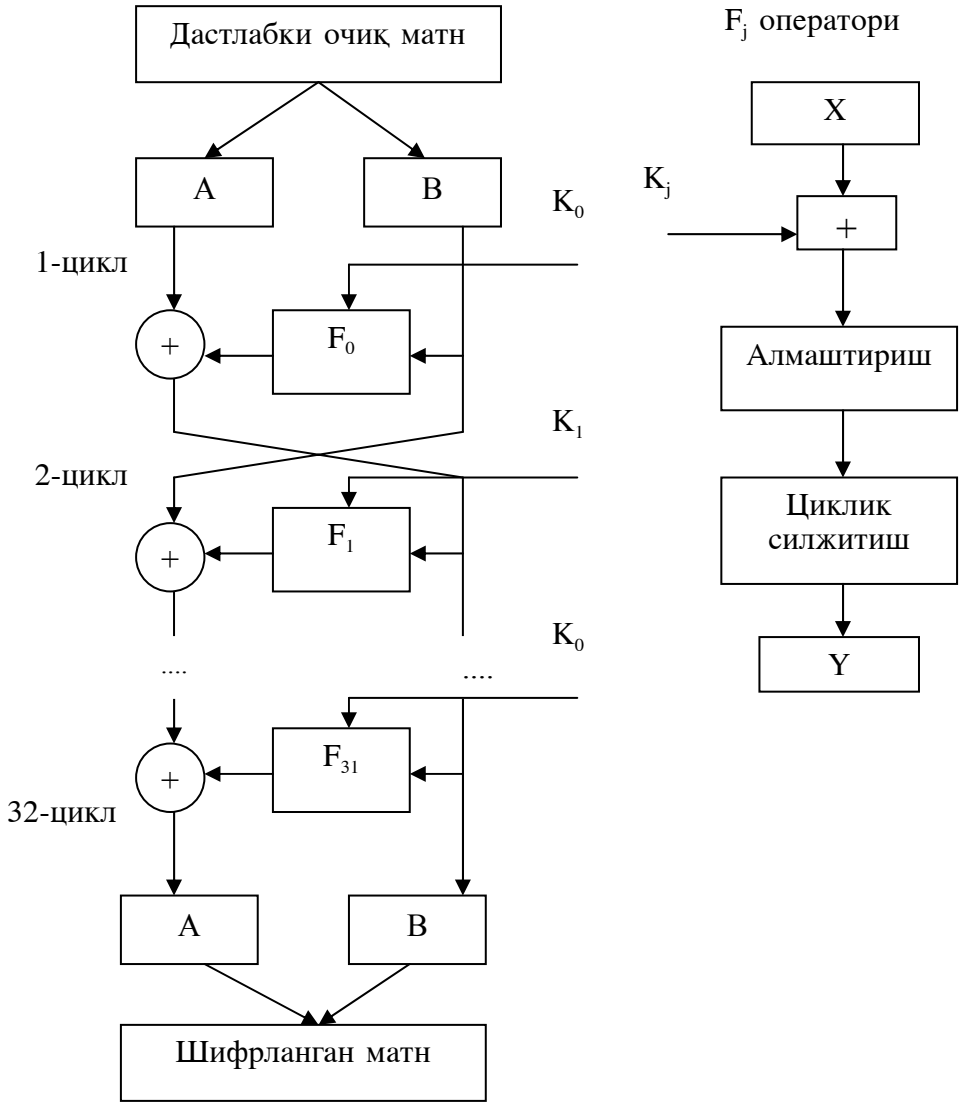
- оддий алмаштириш;
- гаммалаш;
- тескари боғланишли гаммалаш;
- имитовставка.

Бу алгоритмлар учун 8 та 32 хонали иккили сўзларга ажратилган 256 бит ўлчамли калитнинг ишлатилиши ҳамда дастлабки шифрланувчи иккили кетма-кетликнинг 64 битли блокларга ажратилиши умумий ҳисобланади.

Оддий аламштириш алгоритмининг моҳияти қуйидагича (5.12-расм).

Дастлабки кетма-кетликнинг 64 битли блоки иккита 32 хонали A ва B иккили сўзларга ажратилади. A сўзлар блокнинг кичик хоналарини B сўзлар эса катта хоналарини ташкил этади. Бу сўзларга сони i=32 бўлган циклик итерация оператори F_i қўлланилади. Блокнинг кичик битларидаги сўз (биринчи итерациядаги A сўзи) калитининг 32 хонали сўзи билан $\mathrm{mod}2^{32}$ бўйича жамланади; ҳар бири 4 битдан иборат қисмларга (4 хонали кириш йўли векторлари) ажратилади; махсус алмаштириш узеллари ёрдамида ҳар бир вектор бошқаси билан алмаштирилади; олинган векторлар 32 хонали сўзга бирлаштирилиб, чап тарафга циклик равишда силжитилади ва 64 хонали блокдаги бошқа 32 хонали сўз (биринчи итерациядаги B сўзи) билан mod 2 бўйича жамланади.

Биринчи итерация тугаганидан сўнг кичик битлар ўрнида B сўз жойланади, чап тарафда эса A сўз жойланади. Кейинги итерацияларда сўзлар устидаги амаллар такрорланади.



5.12-расм. Оддий алмаштириш алгоритмида шифрлаш жараёнининг блок-схемаси.

Ҳар бир *i*-итерацияда K_j калитнинг (калитлар 8 та) 32 хонали сўзи қуйидаги қоидага биноан танланади

$$K_j = \begin{cases} (i\text{-}1)\ mod\ 8, & 1 \le i \le 24\ бўлганда, \\ 32\text{-}i, & i \ge 25\ бўлганда, \\ 0, & i=32\ бўлганда. \end{cases}$$

$$K_i = \begin{cases} (i-1) \bmod 8, & 1 \le i \le 24 \quad бўлганда, \\ 32-i, & i \ge 25 \quad бўлганда, \\ 0, & i = 32 \quad бўлганда, \end{cases}$$

Демак, шифрлашда калитнинг танланиш тартиби қуйидаги кўринишда бўлади:

K_0,K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7,

K_0,K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_7, K_6, K_5, K_4, K_3, K_2, K_1, K_0,.

Расшифровка қилишда калитлар тескари тартибда ишлатилади.

Алмаштириш блоки кетма-кет танланувчи 8 та алмаштириш узеллари-дан иборат. Алмаштириш узели ҳар бирида алмаштириш вектори (4 бит) жойлашган 16 қаторли жадвалдан иборат. Кириш йўли вектори жадвалдаги қатор адресини аниқласа, қатордаги сон алмаштиришнинг чиқиш йўли вектори ҳисобланади. Алмаштириш жадвалига ахборот олдиндан ёзилади ва камдан-кам ўзгартирилади.

Гаммалаш алгоритмида дастлабки битларнинг кетма-кетлиги гаммаининг битлари кетма-кетлиги билан mod2 бўйича жамланади. Гамма оддий алмаштириш алгоритмига биноан ҳосил қилинади. Гаммани шаклланти-ришда иккита махсус доимийлардан ҳамда 64-хонали иккили кетма-кетилик синхропосилкадан фойдаланилади. Ахборотни фақат синхропосилка борли-гида расшифровка қилиш мумкин.

Синхропосилка махфий бўлмайди ва очиқ ҳолда ҳисоблаш машинаси хотирасида сақланиши ёки алоқа канали орқали узатилиши мумкин.

Тескари боғланишли гаммалаш алгоритми гаммалаш алгоритмидан фақат шифрлаш жараёнининг биринчи қадамидаги ҳаракатлар билан фарқланади.

Имитовставка нотўғри ахборотни зўрлаб киритилишидан ҳимоялашда ишлатилади. Имитовставка дастлабки ахборот ва махфий калитни ўзгартириш функцияси хисобланади. У k бит узунликдаги иккили кетма-кетликдан иборат бўлиб, k нинг қиймати нотўғри ахборотнинг зўрлаб киритилиши эҳтимоллиги $P_{зк}$ билан қуйидаги муносабат билан боғланган.

$$P_{зк}=\frac{1}{2^k}$$

Имитоставкани шакллантириш алгоритми қуйидаги харакатларнинг кетма-кетлигидан иборат. Очиқ ахборот 64 битли $T(i)$ (i=1,2,3,....,m) блок-ларга ажратилади, бу ерда m-шифрланувчи ахборот хажми орқали аниқланади. Биринчи блок $T(1)$ оддий алмаштириш алгоритмининг биринчи 16 итерацияларига биноан ўзгартирилади. Калит сифатида дастлабки ахбо-

рот шифрланишда ишлатиладиган калит олинади. Олинган 64 битли иккили сўз иккинчи блок $T(2)$ билан mod2 бўйича жамланади. $T(1)$ блок устида қандай итерация ўзгартиришлари бажарилган бўлса жамлаш натижаси устида ҳам шундай ўзгартиришлар амалга оширилади ва охирида $T(3)$ блок билан mod2 бўйича жамланади. Бундай харакатлар дастлабки ахборотнинг m-1 блоки бўйича такрорланади. Агар охирги $T(m)$ блок тўлиқ бўлмаса, у 64 хонагача ноллар билан тўлдиради. Бу блок $T(m-1)$ блок ишланиш натижаси билан mod2 бўйича жамланади ва оддий алмаштириш алгоритмининг биринчи 16 итерациялари бўйича ўзгартирилади. Ҳосил бўлган 64 хонали блокдан к бит узунликдаги сўз ажратиб олинади ва бу сўз имитовставка ҳисобланади.

Имитовставка шифрланган ахборотнинг охирига жойлаштирилади. Бу ахборот олингандан сўнг, у расшифровка қилинади. Расшифровка қилинган ахборот бўйича имитовставка аниқланади ва олингани билан солиштирилади. Агар имитовставкалар мос келмаса, расшифровка қилинган ахборот нотўғри деб ҳисобланади.

АҚШнинг ахборотни шифрлаш стандарти. АҚШда давлат стандарти сифатида DES(Data Encryption Standart) стандарти ишлатилган. Бу стандарт асосини ташкил этувчи шифрлаш алгоритми IBM фирмаси томонидан ишлаб чиқилган бўлиб, АҚШ Миллий Хавфсизлик Агентлигининг мутахасислари томонидан текширилгандан сўнг давлат стандарти мақомини олган. DES стандартидан нафақат федерал департаментлар, балки нодавлат ташкилотлар, нафақат АҚШда, балки бутун дунёда фойдаланиб келинган.

DES стандартида дастлабки ахборот 64 битли блокларга ажратилади ва 56 ёки 64 битли калит ёрдамида криптографик ўзгартирилади.

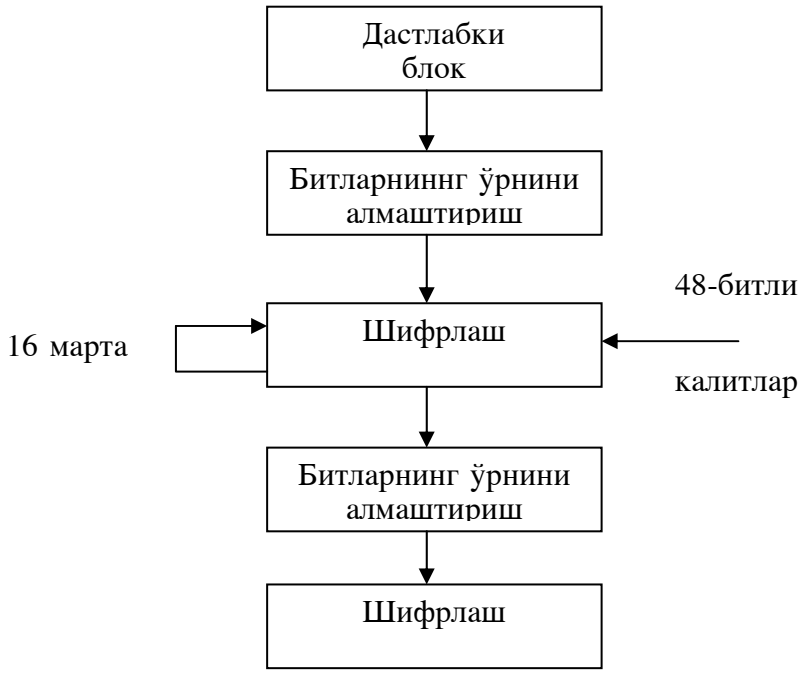
Дастлабки ахборот блоклари ўрин алмаштириш ва шифрлаш функциялари ёрдамида итерацион ишланади. Шифрлаш функциясини ҳисоблаш учун 64 битли калитдан 48 битлигини олиш, 32-битли кодни 48 битли кодга кенгайтириш, 6-битли кодни 4-битли кодга ўзгартириш ва 32-битли кетма-кетликнинг ўрнини алмаштириш кўзда тутилган.

DES алгоритмидаги шифрлаш жараёнининг блок-схемаси 5.13–расмда келтирилган.

Расшифровка жараёни шифрлаш жараёнига инверс бўлиб, шифрлашда ишлатиладиган калит ёрдамида амалга оширилади.

Ҳозирда бу стандарт қуйидаги иккита сабабга кўра фойдаланишга бутунлай яроқсиз ҳисобланади:

- калитнинг узунлиги 56 битни ташкил этади, бу ЭҲМлар-нинг замонавий ривожи учун жуда кам;
- алгоритм яратилаётганида унинг аппарат усулда амалга оширилиши кўзда тутилган эди, яъни алгоритмда микропроцессорларда бажарилишида кўп вақт талаб қилувчи амаллар бор эди (масалан, машина сўзида маълум схема бўйича битларнинг ўрнини алмаштириш каби).



5.13.- расм. DES алгоритмида шифрлаш жараёнининг блок-схемаси

Бу сабаблар АҚШ стандартлаш институтининг 1997 йилда симметрик алгоритмнинг янги стандартига танлов эълон қилишига олиб келди. Танлов шартларига биноан алгоритмга қуйидаги талаблар қўйилган эди:

- алгоритм симметрик бўлиши керак;
- алгоритм блокли шифр бўлиши керак;
- блок узунлиги 128 бит бўлиб, 128, 192, ва 256 битли калит узунликларини таъминлаши лозим.

Ундан ташқари танловда иштирок этувчилар учун қуйидаги тавсиялар берилган эди:

• ҳам аппарат усулда ҳам программ усулда осонгина амалга оширилувчи амаллардан фойдаланиш;

• 32 хонали процессорлардан фойдаланиш;

• иложи борича шифр тузилмасини мураккаблаштирмаслик. Бу ўз навбатида барча қизиқувчиларнинг алгоритмни мустақил тарзда криптотахлил қилиб, унда қандайдир хужжатсиз имкониятлар йўқлигига ишонч ҳосил қилишлари учун зарур ҳисобланади.

2000 йил 2 октябрда танлов натижаси эълон қилинди. Танлов Ғолиби деб Бельгия алгоритми RIJNDAEL топилди ва шу ондан бошлаб алгоритм-Ғолибдан барча патент чегараланишлари олиб ташланди.

Ҳозирда AES (Advanced Encryption Standard) деб аталувчи ушбу алгоритм Дж.Деймен (J. Daemen) ва В. Райджмен (V.Rijmen) томонидан яратилган. Бу алгоритм ноанъанавий блокли шифр бўлиб, кодланувчи маълумотларнинг ҳар бир блоки қабул қилинган блок узунлигига қараб 4x4, 4x6 ёки 4x8 ўлчамдаги байтларнинг икки ўлчамли массивлари кўринишига эга.

Шифрдаги барча ўзгартиришлар қатъий математик асосга эга. Амалларнинг тузилмаси ва кетма-кетлиги алгоритмнинг ҳам 8-битли, ҳам 32-битли микропроцессорларда самарали бажарилишига имкон беради. Алгоритм тузилмасида баъзи амалларнинг параллел ишланиши ишчи станцияларида шифрлаш тезлигининг 4 марта ошишига олиб келади.

Ўзбекистоннинг ахборотни шифрлаш стандарти. Ушбу "Маълумотларни шифрлаш алгоритми" стандарти Ўзбекистон алоқа ва ахборотлаштириш агентлигининг илмий-техник ва маркетинг тадқиқотлари маркази томонидан ишлаб чиқилган ва унда Ўзбекистон Республикасининг "Электрон рақамли имзо хусусида"ги ва "Электрон хужжат алмашинуви хусусида"ги қонунларининг меъёрлари амалга оширилган.

Ушбу стандарт – криптографик алгоритм, электрон маълумотларни ҳимоялашга мўлжалланган. Маълумотларни шифрлаш алгоритми симметрик блокли шифр бўлиб, ахборотни шифрлаш ва расшифровка қилиш учун ишлатилади. Алгоритм 128 ёки 256 бит узунлигидаги маълумотларни

шифрлашда ва расшифровка қилишда 128, 256, 512 битли калитлардан фойдаланиши мумкин.

Стандарт ЭҲМ тармоқларида, телекоммуникацияда, алоҳида ҳисоблаш комплекслари ва ЭҲМда ахборотни ишлаш тизимлари учун ахборотни шифрлашнинг умумий алгоритмини ва маълумотларни шифрлаш қоидасини белгилайди.

Шифрлаш алгоритми дастурий ва аппарат усулларда амалга оширилиши мумкин.

Симметрик шифрлашнинг барча тизимлари қуйидаги камчиликларга эга:

- ахборот алмашувчи икала субъект учун махфий калитни узатиш каналининг ишончлилиги ва хавфсизлигига қуйиладиган талабларнинг қатъийлиги;
- калитларни яратиш ва тақсимлаш хизматига қуйиладиган талабларнинг юқорилиги. Сабаби, ўзаро алоқанинг «ҳар ким – хар ким билан» схемасида «n» та абонент учун $n(n-1)/2$ та калит талаб этилади, яъни калитлар сонининг абонентлар сонига боғлиқлиги квадратли. Масалан, n=1000 абонент учун талаб қилинадиган калитлар сони $n(n-1)/2$=499500. Шу сабабли, фойдаланувчилари юз миллиондан ошиб кетган «Internet» тармоғида симметрик шифрлаш тизимини қўшимча усул ва воситаларсиз қўллашнинг иложи йўқ.

Асимметрик шифрлашнинг биринчи ва кенг тарқалган криптоалгоритми RSA (5.3 га қаралсин) 1993 йилда стандарт сифатида қабул қилинди. Ушбу криптоалгоритм ҳар тарафлама тасдиқланган ва калитнинг етарли узунлигида бардошлиги эътироф этилган. Ҳозирда 512 битли калит бардошликни таъминлашда етарли ҳисобланмайди ва 1024 битли калитдан фойдаланилади. Баъзи муаллифларнинг фикрича процессор қувватининг ошиши RSA криптоалгоритмининг тўлиқ саралаш хужумларга бардошлигининг йўқолишига олиб келади. Аммо, процессор қувватининг ошиши янада узун калитлардан фойдаланишга, ва демак, RSA бардошлигини ошишига имкон яратади.

Асимметрик криптоалгоритмларда симметрик криптоалгоритмлардаги камчиликлар бартарф этилган:

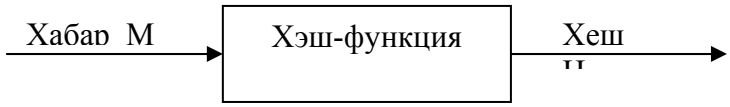
- калитларни маҳфий тарзда етказиш зарурияти йўқ; асимметрик шифрлаш очиқ калитларни динамик тарзда етказишга имкон беради, симметрик шифрлашда эса ҳимояланган алоқа сеанси бошланишидан аввал маҳфий калитлар алмашиниши зарур эди;
- калитлар сонининг фойдаланувчилар сонига квадратли боғланишлиги йўқолади; RSA асимметрик криптотизимда калитлар сонининг фойдаланувчилар сонига боғлиқлиги чизиқли кўринишга эга (*N* фойдаланувчиси бўлган тизимда 2*N* калит ишлатилади).

Аммо асимметрик криптотизимлар, хусусан RSA криптотизими, камчиликлардан ҳоли эмас:

- ҳозиргача асимметрик алгоритмларда ишлатилувчи функцияларнинг қайтарилмаслигининг математик исботи йўқ;
- асимметрик шифрлаш симметрик шифрлашга нисбатан секин амалга оширилади, чунки шифрлашда ва расшифровка қилишда катта ресурс талаб этиладиган амаллар ишлатилади (хусусан, RSAда катта сонни катта сонли даражага ошириш талаб этилади). Шу сабабли асимметрик алгоритмларни аппарат амалга оширилиши, симметрик алгоритмлардагига нисбатан анчагина мураккаб;
- очиқ калитларни алмаштириб қуйилишидан ҳимоялаш зарур. Фараз қилайлик "*A*" абонентнинг компьютерида "*B*" абонентнинг очиқ калити "K_B" сақланади. "*n*" нияти бузуқ одам "*A*" абонентда сақланаётган очиқ калитлардан фойдалана олади. У ўзининг жуфт (очиқ ва махфий) "K_n" ва "k_n" калитларини яратади ва "*A*" абонентда сақланаётган "*B*" абонентнинг "K_B" калитини ўзининг очиқ "K_n" калити билан алмаштиради. "*A*" абонент қандайдир ахборотни "B" абонентга жўнатиш учун уни "K_n" калитда (бу "K_B" калит деб ўйлаган ҳолда) шифрлайди. Натижада, бу хабарни "*B*" абонент ўқий олмайди, "*n*" абонент осонгина расшифровка қилади ва ўқийди. Очиқ калитларни алмаштиришни олдини олишда калитларни сертификациялашдан фойдаланилади.

5.5. Хэшлаш функцияси

Хэшлаш функцияси (хэш-функцияси) шундай ўзгартиришки, кириш йўлига узунлиги ўзгарувчан хабар *M* берилганида чиқиш йўлида белгиланган узунликдаги қатор *h*(*M*) ҳосил бўлади. Бошқача айтганда, хеш-функция *h*(.) аргумент сифатида узунлиги ихтиёрий хабар (хужжат) *M* ни қабул қилади ва белгиланган узунликдаги хеш-қиймат (хеш) *H*=*h*(*M*)ни қайтаради (5.14-расм).



5.14-расм. Хэшни шакллантириш схемаси

Хэш-қиймат h(M) – хабар M нинг дайджести, яъни ихтиёрий узунликдаги асосий хабар *M*нинг хичлантирилган иккилик ифодаси. Хэшлаш функцияси ўлчами мегабайт ва ундан катта бўлган имзо чекилувчи хужжат *M*ни 128 ва ундан катта битга (хусусан, 128 ёки 256 бит) зичлаштиришга имкон беради. Таъкидлаш лозимки, хеш-функция *h(M)* қийматининг хужжат *M*га боғлиқлиги мураккаб ва хужжат *M*нинг ўзини тиклашга имкон бермайди.

Хэшлаш функцияси қуйидаги хусусиятларга эга бўлиши лозим:

1. Хэш-функция ихтиёрий ўлчамли аргументга қўлланиши мумкин.
2. Хэш-функция чиқиш йўлининг қиймати белгиланган ўлчамга эга.
3. Хэш-функция *h*(*x*) ни ихтиёрий *"x"* учун етарлича осон ҳисобланади. Хэш-функцияни ҳисоблаш тезлиги шундай бўлиши керакки, хэш-функция ишлатилганида электрон рақамли имзони тузиш ва текшириш тезлиги хабарнинг ўзидан фойдаланилганига қараганда анчагина катта бўлсин.
4. Хэш-функция матн *M* даги орасига қўйишлар (вставки), чиқариб ташлашлар (выбросы), жойини ўзгартиришлар ва ҳ. каби ўзгаришларга сезгир бўлиши лозим.
5. Хэш-функция қайтарилмаслик хусусиятига эга бўлиши лозим.

6. Иккита турли хужжатлар (уларнинг узунлигига боғлиқ бўлмаган ҳолда) хэш-функциялари қийматларининг мос келиши эҳтимоллиги жуда кичкина бўлиши шарт, яъни ҳисоблаш нуқтаи назаридан $h(x')=h(x)$ бўладиган $x' \neq x$ ни топиш мумкин эмас.

Иккита турли хабар бита тугунчага (свертка) зичлаштириш назарий жиҳатдан мумкин. Бу коллизия ёки тўқнашиш деб аталади. Шунинг учун хэшлаш функциясининг бардошлигини таъминлаш мақсадида тўқнашишларга йўл қўймасликни кўзда тутиш лозим. Тўқнашишларга бутунлай йўл қўймаслик мумкин эмас, чунки умумий ҳолда мумкин бўлган хабарлар сони хэшлаш функциялари чиқиш йўллари қийматларининг мумкин бўлган сонидан ортиқ. Аммо, тўқнашишлар эҳтимоллиги паст бўлиши лозим.

5-хусусият $h(.)$ бир томонлама эканлигини билдирса, 6 хусусият бир бир хил тугунчани берувчи иккита ахборотни топиш мумкин эмаслигини кафолатлайди. Бу сохталаштиришни олдини олади.

Шундай қилиб, хэшлаш функциясидан хабар ўзгаришини пайқашда фойдаланиш мумкин, яъни у *криптографик назорат йиғиндисини* (ўзгаришларни пайқаш коди ёки *хабарни аутентификациялаш коди* деб ҳам юритилади) шакллантиришга хизмат қилиши мумкин. Бу сифатда хэш-функция хабарнинг яхлитлигини назоратлашда, электрон рақамли имзони шакллантаришда ва текширишда ишлатилади.

Хэш-функция фойдаланувчини аутентифкациялашда ҳам кенг қўлланилади. Ахборот хавфсизлигининг қатор технологияларида шифрлашнинг ўзига хос усули *бир томонлама хеш-функция ёрдамида шифрлаш* ишлатилади. Бу шифрлашнинг ўзига хослиги шундан иборатки, у моҳияти бўйича, бир томонламадир, яъни тескари муолажа – қабул қилувчи томонда расшифровка қилиш билан бирга олиб борилмайди. Иккала тараф (жўнатувчи ва қабул қилувчи) хэш-функция асосидаги бир томонлама шифрлаш муолажасидан фойдаланади.

Энг оммабоп хэш-функциялар – MD2, MD4, MD5 ва SHA.

MD2, MD4 ва MD5 – Р.Райвест томонидан ишлаб чиқилган ахборот дайджестини ҳисобловчи алгоритм. Уларнинг ҳар бири 128 битли хэш-

кодни тўзади. MD2 алгоритми энг секин ишласа, MD4 алгоритми тезкор ишлайди. MD5 алгоритми MD4 алгоритмининг модификацияси бўлиб, MD4 алгоритмида хавфсизликнинг оширилиши эвазига тезликдан ютқазилган. SHA(Secure Hash Algorithm) – 160 битли *хэш-код*ни тузувчи ахборот дайджестини ҳисобловчи алгоритм. Бу алгоритм MD4 ва MD5 алгоритмларига нисбатан ишончлироқ.

5.6. Электрон рақамли имзо

Электрон хужжатларни тармоқ орқали алмашишда уларни ишлаш ва сақлаш харажатлари камаяди, қидириш тезлашади.Аммо, электрон хужжат муаллифини ва хужжатнинг ўзини аутентификациялаш, яъни муаллифнинг хақиқийлигини ва олинган электрон хужжатда ўзгаришларнинг йўқлигини аниқлаш муаммоси пайдо бўлади.

Электрон хужжатларни ауентификациялашдан мақсад уларни мумкин бўлган жинояткорона харакатлардан ҳимоялашдир. Бундай харакатларга қуйидагилар киради:

- *фаол ушлаб қолиш* - тармоққа уланган бузғунчи хужжатларни (файлларни) ушлаб қолади ва ўзгартиради.

- *маскарад* – абонент *C* хужжатларни абонент *B* га абонент *A* номидан юборади;

- *ренегатлик* – абонент *A* абонент *B* га хабар юборган бўлсада, юбормаганман дейди;

- *алмаштириш* – абонент *B* хужжатни ўзгартиради, ёки янгисини шакиллантирадива уни абонент *A* дан олганман дейди;

- *такрорлаш* – абонент *A* абонент *B* га юборган хужжатни абонент *C* такрорлайди.

Жинояткорона харакатларнинг бу турлари ўз фаолиятида компьютер ахборот технологияларидан фойдаланувчи банк ва тижорат тузилмаларига, давлат корхона ва ташкилотларига хусусий шахсларга анча- мунча зарар етказиши мумкин.

Электрон рақамли имзо методологияси хабар яхлитлигини ва хабар муаллифининг хақиқийлигини текшириш муаммосини самарали ҳал этишга имкон беради.

Электрон рақамли имзо телекоммуникация каналлари орқали узатилувчи матнларни аутентификациялаш учун ишлатилади. Рақамли имзо ишлаши бўйича оддий қўлёзма имзога ўхшаш бўлиб, қуйидаги афзалликларга эга:

- имзо чекилган матн имзо қўйган шахсга тегишли эканлигини тасдиқлайди;

- бу шахсга имзо чекилган матнга боғлиқ мажбуриятларидан тониш имкониятини бермайди;

- имзо чекилган матн яхлитлигини кафолатлайди.

Электрон рақамли имзо-имзо чекилувчи матн билан бирга узатилувчи қўшимча рақамли хабарнинг нисбатан катта бўлмаган сонидир.

Электрон рақамли имзо асимметрик шифрларнинг қайтарувчанлигига ҳамда хабар таркиби, имзонинг ўзи ва калитлар жуфтининг ўзаро боғлиқлигига асосланади. Бу элементларнинг хатто бирининг ўзгариши рақамли имзонинг ҳақиқийлигини тасдиқлашга имкон бермайди. Электрон рақамли имзо шифрлашнинг асимметрик алгоритмлари ва хеш–функциялари ёрдамида амалга оширилади.

Электрон рақамли имзо тизимининг қўлланишида бир- бирига имзо чекилган электрон хужжатларни жўнатувчи абонент тармоғининг мавжудлиги фараз қилинади. Ҳар бир абонент учун жуфт – маҳфий ва очиқ калит генерацияланади. Маҳфий калит абонентда сир сақланади ва ундан абонент электрон рақамли имзони шакллантиришда фойдаланади.

Очиқ калит бошқа барча фойдаланувчиларга маълум бўлиб, ундан имзо чекилган электрон хужжатни қабул қилувчи электрон рақамли имзони текширишда фойдаланади.

Электрон рақамли имзо тизими иккита асосий муолажани амалга оширади:

- рақамли имзони шакллантириш муолажаси;

- рақамли имзони текшириш муолажаси.

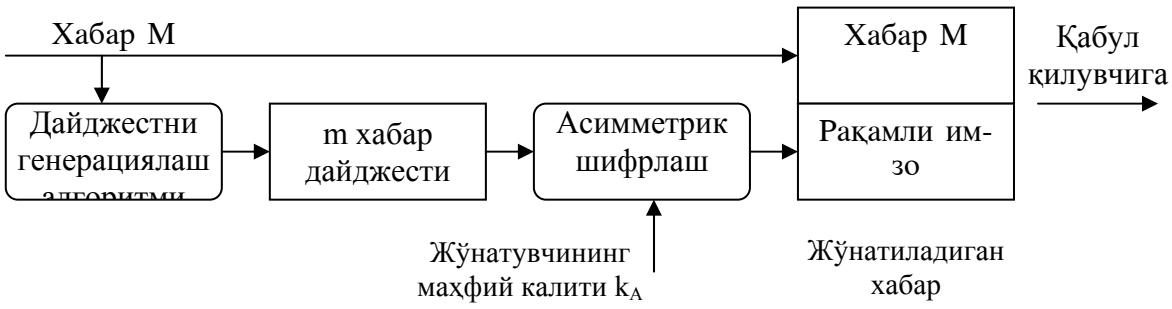
Имзони шакллантириш муолажасида хабар жўнатувчисининг махфий калити ишлатилса, имзони текшириш муолажасида жўнатувчининг очиқ калитидан фойдаланилади.

Рақамли имзони шакллантириш муолажаси.

Ушбу муолажани тайёрлаш босқичида хабар жўнатувчи абонент *A* иккита калитни генерациялайди: маҳфий калит $k_{A.}$ ва очиқ калит K_A. Очиқ калит K_A унинг жуфти бўлган махфий калити $k_{A.}$ дан ҳисоблаш орқали олинади. Очиқ калит K_A тармоқнинг бошқа абонентларига имзони текширишда фойдаланиш учун тарқатилади.

Рақамли имзони шакллантириш учун жўнатувчи *A* аввало имзо чекилувчи матн *M* нинг хеш функцияси *L(M)* қийматини ҳисоблайди (5.15-расм).

Хеш-функция имзо чекилувчи дастлабки матн *“M”* ни дайджест *“m”* га зичлаштиришга хизмат қилади. Дайджест *M*–бутун матн *“M”* ни характерловчи битларнинг белгиланган катта бўлмаган сонидан иборат нисбатан қисқа сондир. Сўнгра жўнатувчи *A* ўзининг маҳфий калити k_A билан дайджест *“m”* ни шифрлайди. Натижада олинган сонлар жуфти берилган *“M”* матн учун рақамли имзо ҳисобланади. Хабар *“M”* рақамли имзо билан биргаликда қабул қилувчининг адресига юборилади.

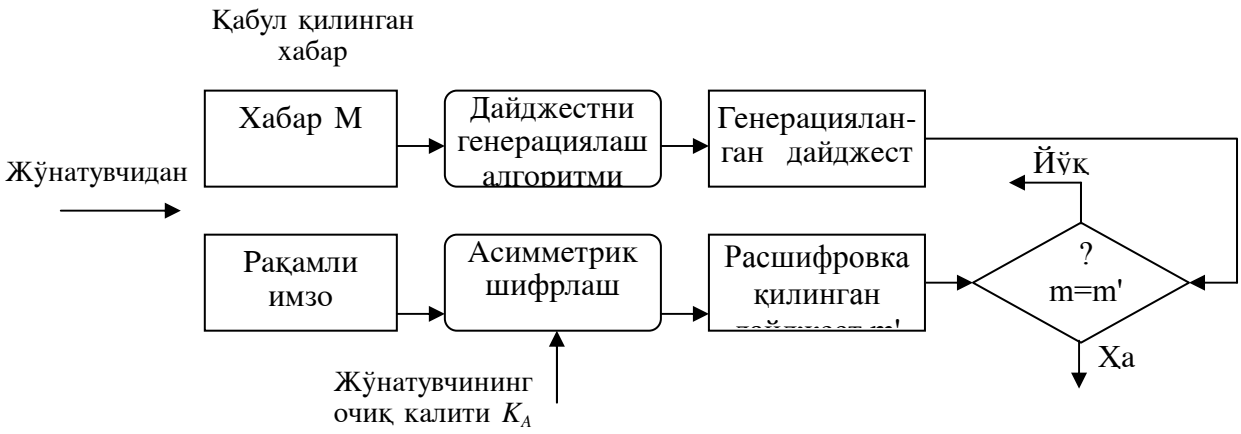


5.15–расм. Электрон рақамли имзони шакллантириш схемаси.

Рақамли имзони текшириш муолажаси.

Тармоқ абонентлари олинган хабар *“M”* нинг рақамли имзосини ушбу хабарни жўнатувчининг очик калити K_A ёрдамида текширишлари мумкин (5.16-расм).

Электрон рақамли имзони текширишда хабар *“M”*ни қабул қилувчи *“B”* қабул қилинган дайджестни жўнатувчининг очиқ калити *“K_A”* ёрдамида расшифровка қилади. Ундан ташқари, қабул қилувчини ўзи хеш-функция *h(M)* ёрдамида қабул қилинган хабар *“M”* нинг дайджести *“m”* ни ҳисоблайди ва уни расшифровка қилингани билан таққослайди. Агар иккала дайджест *“m”* ва *“m'”* мос келса рақамли имзо ҳақиқий ҳисобланади. Акс ҳолда имзо қалбакилаштирилган, ёки ахборот мазмуни ўзгартирилган бўлади.



5.16–расм. Электрон рақамли имзони текшириш схемаси.

Электрон рақамли имзо тизимининг принципиал жиҳати– фойдаланувчининг электрон рақамли имзосини унинг имзо чекишдаги махфий калитини билмасдан қалбакилаштиришнинг мумкин эмаслигидир. Шунинг учун имзо чекишдаги махфий калитни рухсатсиз фойдаланишдан химоялаш зарур. Электрон рақамли имзонинг махфий калитини, симметрик шифрлаш калитига ўхшаб, шахсий калит элитувчисида, ҳимояланган ҳолда сақлаш тавфсия этилади.

Электрон рақамли имзо имзо чекилувчи хужжат ва махфий калит орқали аниқланувчи ноёб сондир. Имзо чекилувчи хужжат сифатида ҳар қандай файл ишлатилиши мумкин. Имзо чекилган файл имзо чекилмаганига бир ёки бир нечта электрон имзо қўшилиши орқали яратилади.

Имзо чекилувчи файлга жойлаштирилувчи электрон рақамли имзо имзо чекилган хужжат муаллифини идентификацияловчи қўшимча ахборот-

га эга. Бу ахборот хужжатга электрон рақамли имзо ҳисобланмасидан олдин қўшилади. Ҳар бир имзо қуйидаги ахборотни ўз ичига олади:

- имзо чекилган сана;

- ушбу имзо калити таъсирининг тугаши муддати;

- файлга имзо чекувчи шахс хусусидаги ахборот (Ф.И.Ш., мансаби, иш жойи);

- имзо чекувчининг индентификатори (очиқ калит номи);

- рақамли имзонинг ўзи.

Асимметрик шифрлашга ўхшаш, электрон рақамли имзони текшириш учун ишлатиладиган очиқ калитнинг алмаштирилишига йўл қўймаслик лозим. Фараз қилайлик, нияти бузуқ одам "*n*" абонент "*B*" компьютерида сақланаётган очиқ калитлардан, хусусан, абонент *A* нинг очиқ калити K_A дан фойдалана олади. Унда у қуйидаги харакатларини амалга ошириши мумкин:

- очиқ калит K_A сақланаётган файлдан абонент *A* хусусидаги инденцификация ахборотини ўқиши;

- ичига абонент *A* хусусидаги индентификация ахборотини ёзган ҳолда шахсий жуфт калитлари k_n ва K_n ни генерациялаши;

- абонент *B*да сақланаётган очиқ калит K_Aни ўзининг очиқ калити K_n билан алмаштириши.

Сўнгра нияти бузуқ одам "*n*" абонент *B* га хужжатларни ўзининг махфий калити k_n ёрдамида имзо чекиб жўнатиши мумкин. Бу хужжатлар имзосини текширишда абонент *B* абонент *A* имзо чеккан хужжатларни ва уларнинг электрон рақамли имзоларини тўғри ва хеч ким томонидан модификацияланмаган деб ҳисоблайди. Абонент А билан муносабатларини бевосита ойдинлаштирилишигача В абонентда олинган хужжатларнинг хақиқийлигига шубҳа туғилмайди.

Электрон рақамли имзонинг қатор алгоритмлари ишлаб чиқилган. 1977 йилда АҚШ да яратилган RSA тизими биринчи ва дунёда машҳур электрон рақамли имзо тизими ҳисобланади ва юқорида келтирилган принципларни амалга оширади. Аммо рақамли имзо алгоритми RSA жиддий камчиликка эга. У нияти бузуқ одамга махфий калитни билмасдан, хеш-

лаш натижасини имзо чекиб бўлинган хужжатларнинг хешлаш натижаларини кўпайтириш оркали ҳисоблаш мумкин бўлган хужжатлар имзосини шакллантиришга имкон беради.

Ишончлилигининг юқорилиги ва шахсий компьютерларда амалга оширилишининг қулайлиги билан ажралиб турувчи рақамли имзо алгоритмли 1984 йилда Эль Гамал томонидан ишлаб чиқилди. Эль Гамалнинг рақамли имзо алгоритми (EGSA) RSA рақамли имзо алгоритмидаги камчиликлардан ҳоли бўлиб, АҚШ нинг стандартлар ва технологияларнинг Миллий университети томонидан рақамли имзонинг миллий стандартига асос каби қабул қилинди.

5.7. Криптографик калитларни бошқариш

Ҳар қандай криптографик тизим крпитографик калитлардан фойдаланишга асосланган. Калит ахбороти деганда ахборот тармоқлари ва тизимларида ишлатилувчи барча калитлар мажмуи тушунилади. Агар калит ахборотларининг етарлича ишончли бошқарилиши таъминланмаса, нияти бузуқ одам унга эга бўлиб олиб тармоқ ва тизимдаги барча ахборотдан ҳоҳлаганича фойдаланиши мумкин. Калитларни бошқариш калитларни генерациялаш, сақлаш ва тақсимлаш каби вазифаларни бажаради. Калитларни тақсимлаш калитларни бошқариш жараёнидаги энг маъсулиятли жараён ҳисобланади.

Симметрик криптотизимдан фойдаланилганда ахборот алмашинувида иштирок этувчи иккала томон аввал махфий сессия калити, яъни алмашинув жараёнида узатиладиган барча хабарларни шифрлаш калити бўйича келишишлари лозим. Бу калитни бошқа барча билмаслиги ва уни вақти-вақти билан жўнатувчи ва қабул қилувчида бир вақтда алмаштириб туриш лозим. Сессия калити бўйича келишиш жараёнини калитларни алмаштириш ёки тақсимлаш деб ҳам юритилади.

Асимметрик криптотизимда иккита калит-очиқ ва ёпиқ (махфий) калит ишлатилади. Очиқ калитни ошкор этиш мумкин, ёпиқ калитни яши-

риш лозим. Хабар алмашинувида фақат очиқ калитни унинг ҳақиқийлигини таъминлаган ҳолда жўнатиш лозим.

Калитларни тақсимлашга қуйидаги талаблар қўйилади:

- тақсимлашнинг оперативлиги ва аниқлиги;
- тақсимланувчи калитларнинг конфиденциаллиги ва яхлитлиги.

Компьютер тармоқларидан фойдаланувчилар ўртасида калитларни тақсимлашнинг қуйидаги асосий усулларидан фойдаланилади.

1. Калитларни тақсимловчи битта ёки бир нечта марказлардан фойдаланиш.
2. Тармоқ фойдаланувчилари ўртасида калитларни тўғридан-тўғри алмашиш.

Биринчи усулнинг муаммоси шундаки, калитларни тақсимлаш марказига кимга, қайси калитлар тақсимланганлиги маълум. Бу эса тармоқ бўйича узатилаётган барча хабарларни ўқишга имкон беради. Бўлиши мумкин бўлган суиистеъмоллар тармоқ хавфсизлигининг жиддий бузилишига олиб келиши мумкин.

Иккинчи усулдаги муаммо – тармоқ субъектларининг ҳақиқий эканлигига ишонч ҳосил қилишдир.

Калитларни тақсимлаш масаласи қуйидагиларни таъминловчи калитларни тақсимлаш протоколини қуришга келтирилади:

- сеанс қатнашчиларининг ҳақиқийлигига иккала томоннинг тасдиғи;
- сеанс ҳақиқийлигининг тасдиғи;
- калитлар алмашинувида хабарларнинг минимал сонидан фойдаланиш.

Биринчи усулга мисол тариқасида Kerberos деб аталувчи калитларни аутентификациялаш ва тақсимлаш тизимини кўрсатиш мумкин.

Иккинчи усулга-тармоқ фойдаланувчилари ўртасида калитларни тўғридан-тўғри алмашишга батафсил тўхталамиз.

Симметрик калитли криптотизимдан фойдаланилганда криптографик ҳимояланган ахборот алмашинувини истаган иккала фойдаланувчи умумий махфий калитга эга бўлишлари лозим. Бу фойдаланувчилар умумий калит-

ни алоқа канали бўйича хавфсиз алмашишлари лозим. Агар фойдаланувчилар калитни тез-тез ўзгартириб турсалар калитни етказиш жиддий муаммога айланади.

Бу муаммони ечиш учун қуйидаги иккита асосий усул қўлланилади:

1. Симметрик криптотизимнинг махфий калитини ҳимоялаш учун очиқ калитли асимметрик криптотизимдан фойдаланиш
2. Диффи-Хеллманнинг калитларни очиқ тақсимлаш тизимидан фойдаланиш.

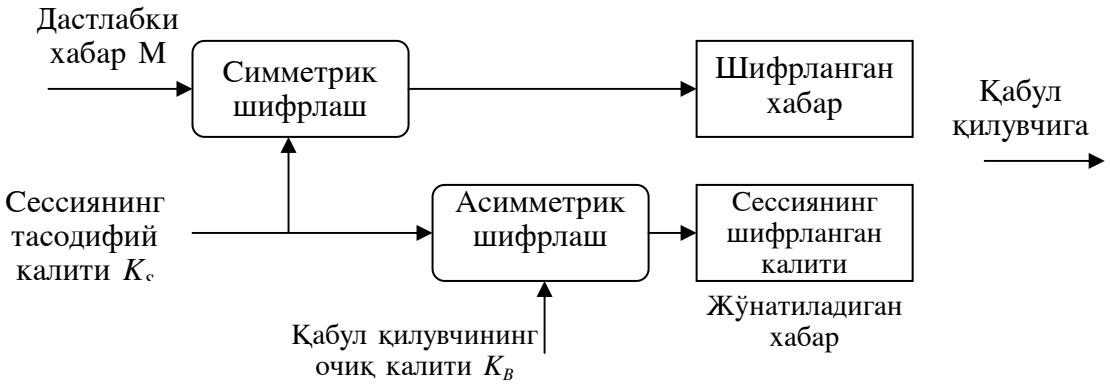
Биринчи усул симметрик ва асимметрик калитли комбинацияланган криптотизим доирасида амалга оширилади. Бундай ёндашишда симметрик криптотизим дастлабки очиқ матнни шифрлаш ва узатишда ишлатилса, очиқ калитли асимметрик криптотизим фақат симметрик криптотизимнинг махфий калитини шифрлаш, узатиш ва кейинги расшифровка қилишда ишлатилади. Шифрлашнинг бундай комбинацияланган (гибрид) усули очиқ калитли асимметрик криптотизимнинг юқори махфийлиги билан махфий калитли симметрик криптотизимнинг юқори тезкорлигининг уйғунлашишга олиб келади. Бундай ёндашиш баъзида *электрон рақамли конверт* схемаси деб юритилади.

Фараз қилайлик, фойдаланувчи A хабар M ни фойдаланувчи B га ҳимояланган узатиш учун шифрлашнинг комбинацияланган усулидан фойдаланмоқчи. Унда фойдаланувчиларнинг ҳаракатлари қуйидагича бўлади.

Фойдаланувчи A нинг ҳаракатлари:

1. Симметрик сеанс махфий калит K_S ни яратади (масалан, тасодифий тарзда генерациялайди).
2. Хабар M ни симметрик сеанс махфий калит K_S да шифрлайди.
3. Махфий сеанс калит K_S ни фойдаланувчи (хабар қабул қилувчи) Bнинг очиқ калити K_B да шифрлайди.
4. Фойдаланувчи B адресига алоқанинг очиқ канали бўйича шифрланган хабар M ни шифрланган сеанс калити K_S билан биргаликда узатади.

Фойдаланувчи *A* нинг харакаталарини 5.17-расмда келтирилган хабарларни комбинацияланган усул бўйича шифрлаш схемаси орқали тушуниш мумкин.

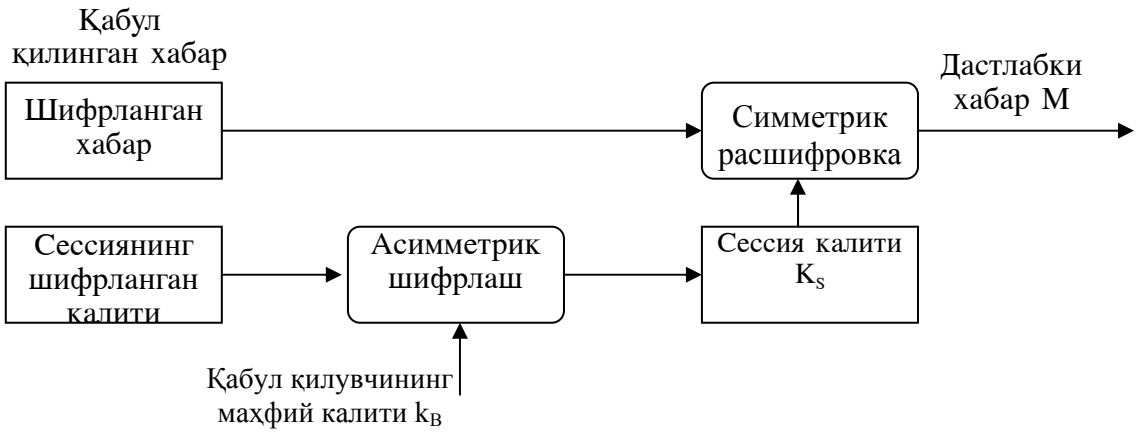


5.17–расм. Комбинацияланган усул бўйича хабарни шифрлаш схемаси.

Фойдаланувчи *B* нинг ҳаракатлари (электрон рақамли конвертни-шифрланган хабар *M* ни ва шифрланган сеанс калити K_S ни олганидан сўнгги) қуйидагича:

1. Ўзининг махфий калити k_B бўйича сеанс калити K_S ни расшифровка қилади.
2. Олинган сеанс калити K_S бўйича олинган хабар *M* ни расшифровка қилади.

Фойдланувчи *B* нинг харакатларини 5.18-расмда келтирилган хабарларни комбинацияланган усул бўйича расшифровка қилиш схемаси орқали тушуниш мумкин.



5.18–расм. Комбинацияланган усул бўйича хабарни расшифровка қилиш.

Олинган электрон рақамли конвертни фақат қонуний қабул қилувчи-фойдаланувчи B очиши мумкин. Фақат шахсий махфий калит k_B эгаси бўлган фойдаланувчи B махфий сеанс калити K_S ни тўғри расшифровка қилиш ва сўнгра бу калит ёрдамида олинган хабар M ни расшифровка қилиши ва ўқиши мумкин.

Рақамли конверт усулида симметрик ва асимметрик криптоалгоритмларнинг камчиликлари қуйидагича компенсацияланади:

- симметрик криптоалгоритм калитларини тарқатиш муаммоси бартараф қилинади, чунки хабарни шифрловчи сеанс калити K_S очиқ канал бўйича шифрланган кўринишда узатилади, калит K_Sни расшифровка қилиш учун асимметрик криптоалгоритмдан фойдаланилади;
- бу ҳолда асимметрик шифрлаш тезкорлигининг секинлиги муаммоси пайдо бўлмайди, чунки асимметрик алгоритм бўйича фақат қисқа калит K_S шифрланади, барча маълумотлар эса тезкор симметрик криптоалгоритм бўйича шифрланади.

Натижада тезкор шифрлаш билан биргаликда калитларнинг қулай тақсимланиши амалга оширилади.

Шифрлашнинг комбинацияланган усулида симметрик ҳам асимметрик криптотизимларнинг криптографик калитларидан фойдаланилади. Равшанки, криптотизимнинг ҳар бир тури учун калитлар узунлигини шундай танлаш лозимки, нияти бузуқ одамга комбинацияланган криптотизим ҳимоясининг ҳар қандай механизмига хужум қилиш бир хил қийинчилик туғдирсин.

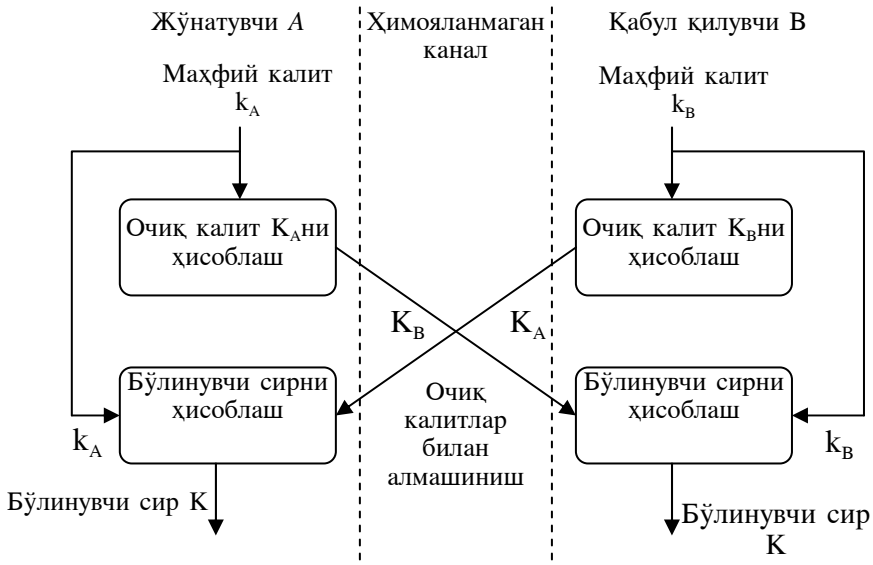
5.1-жадвалда кўп учрайдиган симметрик ва асимметрик криптотизимлар калитларининг узунлиги келтирилган.

5.1-жадвал

Симметрик криптотизим калитлари узунлиги, битлар	Асимметрик криптотизим калитлари узунлиги, битлар
56	384
64	512
80	768
112	1792
128	2304

У. Диффи ва М.Хеллман томонидан кашф этилган *калитларни очиқ тақсимлаш усули* фойдаланувчиларга калитларни ҳимояланмаган алоқа каналлари орқали алмашишга имкон беради. Унинг хавфсизлиги чегараланган соҳада дискрет логарифмларни ҳисоблашнинг мушкуллигига асосланади.

Диффи-Хеллман усулининг моҳияти қуйидагича (5.19-расм).



5.19–расм. Диффи-Хеллманнинг калитларни очиқ тақсимлаш схемаси

Ахборот алмашинувида иштирок этувчи фойдаланувчилар A ва B мустақил равишда ўзларининг махфий калитларини k_A ва k_B ни генерациялайдилар (k_A ва k_B калитлар фойдаланувчилар A ва B лар сир сақловчи тасодифий катта бутун сонлар).

Сўнгра фойдаланувчи A ўзининг махфий калити k_A асосида очиқ калитни ҳисоблайди:

$$K_A = g^{K_A} (\mathrm{mod}\, N).$$

Бир вақтнинг ўзида фойдаланувчи *B* ўзининг махфий калити k_B асосида очиқ калитни ҳисоблайди:

$$K_B = g^{K_B} (\mathrm{mod}\, N).$$

Бу ерда *N* ва *g* – катта бутун оддий сонлар. Арифметик амаллар *N*нинг модулига келтириш орқали бажарилади. *N* ва *g* сонларни сир сақлаш шарт эмас, чунки одатда, бу қийматлар тармоқ ва тизимдан фойдаланувчиларнинг барчаси учун умумий ҳисобланади.

Сўнгра фойдаланувчилар А ва В ўзларининг очиқ калитларини ҳимояланмаган канал орқали алмаштирадилар ва умумий сессия махфий калити *K*ни (бўлинувчи сирни) ҳисоблашда ишлатадилар:

фойдаланувчи А: $K = (K_B)^{k_A} (\mathrm{mod}\, N) = (g^{k_B})^{k_A} (\mathrm{mod}\, N),$

фойдаланувчи В: $K' = (K_A)^{k_B} (\mathrm{mod}\, N) = (g^{k_A})^{k_B} (\mathrm{mod}\, N),$

бунда $K = K'$, чунки $(g^{k_B})^{k_A} = (g^{k_A})^{k_B} (\mathrm{mod}\, N).$

Шундай қилиб, ушбу амаллар натижасида иккала махфий калит k_A ва k_Bларнинг функцияси бўлган умумий сессия махфий калити ҳосил қилинади.

Очиқ калитлар K_A ва K_B қийматларини ушлаб қолган нияти бузуқ одам сессия махфий калити *K* ни ҳисоблай олмайди, чунки у махфий калитлар k_A ва k_B қийматларини билмайди. Бир томонлама функциянинг ишлатилиши сабабли очиқ калитни ҳисоблаш амали қайтарилмайдиган амал, яъни абонентнинг очиқ калити қиймати бўйича унинг махфий калитини ҳисоблаш мумкин эмас.

Диффи-Хеллман усулининг ноёблиги шундан иборатки, абонентлар жуфти тармоқ орқали очиқ калитларни узатганларида фақат ўзларига маълум махфий сонни олиш имкониятига эга. Сўнгра абонентлар узатилаётган ахборотни маълум текширилган усулни – олинган умумий сессия махфий калитидан фойдаланган ҳолда симметрик шифрлашни ишлатиб ҳимоялашга киришишлари мумкин.

Диффи-Хеллман схемаси маълумотларни ҳар бир сеансда янги калитларда шифрлаш имконини беради. Бу сирларни дискетларда ёки бошқа элтувчиларда сақламасликка имкон беради, чунки бундай сақлаш уларни рақиблар ёки нияти бузуқ одамлар қулига тушиб қолиш эҳтимоллигини оширади.

Диффи-Хеллман схемаси *узатилаётган маълумотларнинг конфиденциаллигини ва аутентлигини (аслига тўғрилигини) комплекс ҳимоялаш усули*ни ҳам амалга ошириш имконини беради. Алгоритм фойдаланувчига рақамли имзони ва симметрик шифрлашни бажаришда бир хил калитларни шакллантириш ва ишлатиш имконини беради.

Маълумотлар яхлитлигини ва конфиденциаллигини бир вақтда ҳимоялаш учун шифрлаш ва электрон рақамли имзодан комплекс фойдаланиш мақсадга мувофиқ ҳисобланади. Диффи-Хеллман схемаси ишлашининг оралиқ натижаларидан узатилаётган маълумотларнинг яхлитлигини ва конфиденциаллагини комплекс ҳимоялаш усулини амалга оширишда фойдаланиш мумкин. Ҳақиқатан, ушбу алгоритмга биноан фойдаланувчилар A ва B аввал ўзларининг махфий калитлари k_A ва k_B ни генерациялайдилар ва очиқ калитлари K_A ва K_B ни ҳисоблайдилар. Сўнгра абонентлар A ва B бу оралиқ натижалардан маълумотларни симметрик шифрлашда фойдаланилиши мумкин бўлган умумий бўлинувчи махфий калити K ни бир вақтда ҳисоблаш учун ишлатади.

Узатилаётган маълумотларнинг конфиденциаллигини ва аутентилигини комплекс ҳимоялаш усули қуйидаги схема бўйича ишлайди:

- абонент A рақамли имзонинг стандарт алгоритмидан фойдаланиб, ўзининг махфий калити k_A ёрдамида хабар M га имзо чекади;

- абонент A ўзининг махфий калити k_A ва абонент B нинг очиқ калити K_B дан Диффи-Хеллман алгоритми бўйича умумий бўлинувчи махфий калити K ни ҳисоблайди.

- абонент A олинган ўзаро бўлинувчи махфий калитда алмашинув бўйича шериги билан келишилган симметрик шифрлаш алгоритмидан фойдаланган ҳолда хабар M ни шифрлайди;

- абонент B шифрланган хабар M ни олиши билан ўзининг махфий калити k_B ва абонент A нинг очиқ калити K_A дан Диффи-Хеллман алгоритми бўйича ўзаро бўлинувчи махфий калит K ни ҳисоблайди;

- абонент B олинган хабар M ни калити K да расшифровка қилади;

- абонент B абонент A нинг очиқ калит K_A ёрдамида расшифровка қилинган хабар M имзосини текширади.

Диффи-Хеллман схемаси асосида тармоқ сатҳида ҳимояланган виртуал тармоқлар VPN қурилишида қўлланилувчи криптокалитларни бошқариш протоколлари SKIP (Simple Key Management for Internet Protocols) ва IKE (Internet Key Exchange) ишлайди.

VI боб. ИНДЕНТИФИКАЦИЯ ВА АУТЕНТИФИКАЦИЯ

6.1. Асосий тушунчалар ва туркумланиши

Компьютер тизимида рўйхатга олинган ҳар бир субъект (фойдаланувчи ёки фойдаланувчи номидан ҳаракатланувчи жараён) билан уни бир маънода индентификацияловчи ахборот боғлиқ.

Бу ушбу субъектга ном берувчи сон ёки символлар сатри бўлиши мумкин. Бу ахборот субъект *индентификатори* деб юритилади. Агар фойдаланувчи тармоқда рўйхатга олинган индентификаторга эга бўлса у легал (қонуний), акс ҳолда легал бўлмаган (ноқонуний) фойдаланувчи ҳисобланади. Компьютер ресурсларидан фойдаланишдан аввал фойдаланувчи компьютер тизимининг идентификация ва аутентификация жараёнидан ўтиши лозим.

Идентификация (Identification) - фойдаланувчини унинг идентификатори (номи) бўйича аниқлаш жараёни. Бу фойдаланувчи тармоқдан фойдаланишга уринганида биринчи галда бажариладиган функциядир. Фойдаланувчи тизимга унинг сўрови бўйича ўзининг идентификаторини билдиради, тизим эса ўзининг маълумотлар базасида унинг борлигини текширади.

Аутентификация (Authentication) – маълум қилинган фойдаланувчи, жараён ёки қурилманинг ҳақиқий эканлигини текшириш муолажаси. Бу текшириш фойдаланувчи (жараён ёки қурилма) ҳақиқатан айнан ўзи эканлигига ишонч хосил қилишига имкон беради. Аутентификация ўтқазишда текширувчи тараф текширилувчи тарафнинг хақиқий эканлигига ишонч ҳосил қилиши билан бир қаторда текширилувчи тараф ҳам ахборот алмашинув жараёнида фаол қатнашади. Одатда фойдаланувчи тизимга ўз хусусидаги ноёб, бошқаларга маълум бўлмаган ахборотни (масалан, парол ёки сертификат) киритиши орқали идентификацияни тасдиқлайди.

Идентификация ва аутентификация субъектларнинг (фойдаланувчиларнинг) ҳақиқий эканлигини аниқлаш ва текширишнинг ўзаро боғланган жараёнидир. Муайян фойдаланувчи ёки жараённинг тизим ресурсларидан фойдаланишига тизимнинг рухсати айнан шуларга боғлиқ. Субъектни

идентификациялаш ва аутентификациялашдан сўнг уни авторизациялаш бошланади.

Авторизация (Authorization) – субектга тизимда маълум ваколат ва ресурсларни бериш муолажаси, яъни авторизация субъект ҳаракати доирасини ва у фойдаланадиган ресурсларни белгилайди. Агар тизим авторизацияланган шахсни авторизацияланмаган шахсдан ишончли ажрата олмаса бу тизимда ахборотнинг конфиденциаллиги ва яхлитлиги бузилиши мумкин. Аутентификация ва авторизация муолажалари билан фойдаланувчи ҳаракатини маъмурлаш муолажаси узвий боғланган.

Маъмурлаш (Accounting) – фойдаланувчининг тармоқдаги ҳаракатини, шу жумладан, унинг ресурслардан фойдаланишга уринишини қайд этиш. Ушбу ҳисобот ахбороти хавфсизлик нуқтаи назаридан тармоқдаги хавфсизлик ходисаларини ошкор қилиш, тахлиллаш ва уларга мос реакция кўрсатиш учун жуда муҳимдир.

Маълумотларни узатиш каналларини ҳимоялашда *субъектларнинг ўзаро аутентификацияси*, яъни алоқа каналлари орқали боғланадиган субъектлар хақиқийлигининг ўзаро тасдиғи бажарилиши шарт. Хақиқийликнинг тасдиғи одатда сеанс бошида, абонентларнинг бир-бирига уланиш жараёнида амалга оширилади. “Улаш” атамаси орқали тармоқнинг иккита субъекти ўртасида мантиқий боғланиш тушунилади. Ушбу муолажанинг мақсади – улаш қонуний субъект билан амалга оширилганлигига ва барча ахборот мўлжалланган манзилга боришлигига ишончни таъминлашдир.

Ўзининг хақиқийлигининг тасдиқлаш учун субъект тизимга турли асосларни кўрсатиши мумкин. Субъект кўрсатадиган асосларга боғлиқ ҳолда аутентификация жараёнлари қуйидаги категорияларга бўлиниши мумкин:

- *бирор нарсани билиш асосида.* Мисол сифатида парол, шахсий идентификация коди PIN (Personal Identification Number) ҳамда “сўров жавоб” хилидаги протоколларда намойиш этилувчи махфий ва очиқ калитларни кўрсатиш мумкин;

- *бирор нарсага эгалиги асосида.* Одатда булар магнит карталар, смарт-карталар, сертификатлар ва touch memory қурилмалари;

- *қандайдир дахлсиз характеристикалар асосида.* Ушбу категория ўз таркибига фойдаланувчининг биометрик характеристикаларига (овозлар, кўзининг рангдор пардаси ва тўр пардаси, бармоқ излари, кафт геометрияси ва х.) асосланган усулларни олади. Бу категорияда криптографик усуллар ва воситалар ишлатилмайди. Беометрик характеристикалар бинодан ёки қандайдир техникадан фойдаланишни назоратлашда ишлатилади.

Парол – фойдаланувчи ҳамда унинг ахборот алмашинувидаги шериги биладиган нарса. Ўзаро аутентификация учун фойдаланувчи ва унинг шериги ўртасида парол алмашиниши мумкин. Пластик карта ва смарт-карта эгасини аутентификациясида шахсий идентификация номери PIN синалган усул ҳисобланади. PIN – коднинг маҳфий қиймати фақат карта эгасига маълум бўлиши шарт.

Динамик – (бир марталик) парол - бир марта ишлатилганидан сўнг бошқа умуман ишлатилмайдиган парол. Амалда одатда доимий паролга ёки таянч иборога асосланувчи мунтазам ўзгариб турувчи қиймат ишлатилади.

“Сўров-жавоб” тизими - тарафларнинг бири ноёб ва олдиндан билиб бўлмайдиган “сўров” қийматини иккинчи тарафга жўнатиш орқали аутентификацияни бошлаб беради, иккинчи тараф эса сўров ва сир ёрдамида ҳисобланган жавобни жўнатади. Иккала тарафга битта сир маълум бўлгани сабабли, биринчи тараф иккинчи тараф жавобини тўғрилигини текшириши мумкин.

Сертификатлар ва рақамли имзолар - агар аутентификация учун сертификатлар ишлатилса, бу сертификатларда рақамли имзонинг ишлатилиши талаб этилади. Сертификатлар фойдаланувчи ташкилотининг масъул шахси, сертификатлар сервери ёки ташқи ишончли ташкилот томонидан берилади. Internet доирасида очиқ калит сертификатларини тарқатиш учун очиқ калитларни бошқарувчи қатор тижорат инфратузилмалари PKI (Public Key Infrastructure) пайдо бўлди. Фойдаланувчилар турли даража сертификатларини олишлари мумкин.

Аутентификация жарёнларини таъминланувчи хавфсизлик даражаси бўйича ҳам туркумлаш мумкин. Ушбу ёндашишга биноан аутентификация жараёнлари қуйидаги турларга бўлинади:

- пароллар ва рақамли сертификатлардан фойдаланувчи аутентификация;
- криптографик усуллар ва воситалар асосидаги қатьий аутентификация;
- нуллик билим билан исботлаш хусусиятига эга бўлган аутентификация жараёнлари (протоколлари);
- фойдаланувчиларни биометрик аутентификацияси.

Хавфсизлик нуқтаи назаридан юқорида келтирилганларнинг ҳар бири ўзига хос масалаларни ечишга имкон беради. Шу сабабли аутентификация жараёнлари ва протоколлари амалда фаол ишлатилади. Шу билан бир қаторда таъкидлаш лозимки, нуллик билим билан исботлаш хусусиятига эга бўлган аутентификацияга қизиқиш амалий характерга нисбатан кўпроқ назарий характерга эга. Балким, яқин келажакда улардан ахборот алмашинувини ҳимоялашда фаол фойдаланишлари мумкин.

Аутентификация протоколларига бўладиган асосий хужумлар қуйидагилар:

- *маскарад* (impersonation). Фойдаланувчи ўзини бошқа шахс деб кўрсатишга уриниб, у шахс тарафидан харакатларнинг имкониятларига ва имтиёзларига эга бўлишни мўлжаллайди;
- аутентификация алмашинуви *тарафини алмаштириб қўйиш* (interleaving attack). Нияти бузуқ одам ушбу хужум мобайнида икки тараф орасидаги аутенфикацион алмашиниш жараёнида трафикни модификациялаш ниятида қатнашади. Алмаштириб қўйишнинг қуйидаги хили мавжуд: иккита фойдаланувчи ўртасидаги аутентификация муваффақиятли ўтиб, уланиш ўрнатилганидан сўнг бузғунчи фойдаланувчилардан бирини чиқариб ташлаб, унинг номидан ишни давом эттиради;
- *такрорий узатиш* (replay attack). Фойдаланувчиларнинг бири томонидан аутентификация маълумотлари такроран узатилади;

- *узатишни қайтариш* (reflection attak). Олдинги хужум вариантларидан бири бўлиб, хужум мобайнида нияти бузуқ одам протоколнинг ушбу сессия доирасида ушлаб қолинган ахборотни орқага қайтаради.

- *мажбурий кечикиш* (forced delay). Нияти бузуқ одам қандайдир маълумотни ушлаб қолиб, бирор вақтдан сўнг узатади.

- *матн танлашли хужум* (chosen text attack). Нияти бузуқ одам аутентификация трафигини ушлаб қолиб, узоқ муддатли криптографик калитлар хусусидаги ахборотни олишга уринади.

Юқорида келтирилган хужумларни бартараф қилиш учун аутентификация протоколларини қуришда қуйидаги усуллардан фойдаланилади:

- “сўров–жавоб”, вақт белгилари, тасодифий сонлар, индентификаторлар, рақамли имзолар каби механизмлардан фойдаланиш;

- аутентификация натижасини фойдаланувчиларнинг тизим доирасидаги кейинги харакатларига боғлаш. Бундай мисол ёндашишга тариқасида аутентификация жараёнида фойдаланувчиларнинг кейинга ўзаро алоқаларида ишлатилувчи махфий сеанс калитларини алмашишни кўрсатиш мумкин;

- алоқанинг ўрнатилган сеанси доирасида аутентификация муолажасини вақти-вақти билан бажариб туриш ва ҳ.

“Сўров-жавоб” механизми қуйидагича. Агар фойдаланувчи *A* фойдаланувчи *B* дан оладиган хабари ёлғон эмаслигига ишонч хосил қилишни истаса, у фойдаланувчи *B* учун юборадиган хабарга олдиндан билиб бўлмайдиган элемент – *X* сўровини (масалан, қандайдир тасодифий сонни) қўшади. Фойдаланувчи В жавоб беришда бу амал устида маълум амални (масалан, қандайдир *f(X)* функцияни ҳисоблаш) бажариши лозим. Буни олдиндан бажариб бўлмайди, чунки сўровда қандай тасодифий сон *X* келиши фойдаланувчи *B* га маълум эмас. Фойдаланувчи *B* ҳаракати натижасини олган фойдаланувчи *A* фойдаланувчи *B* нинг хақиқий эканлигига ишонч хосил қилиши мумкин. Ушбу усулнинг камчилиги - сўров ва жавоб ўртасидаги қонуниятни аниқлаш мумкинлиги.

Вақтни белгилаш механизми ҳар бир хабар учун вақтни қайдлашни кўзда тутади. Бунда тармоқнинг ҳар бир фойдаланувчиси келган хабарнинг қанчалик эскирганини аниқлаши ва уни қабул қилмаслик қарорига келиши мумкин, чунки у ёлғон бўлиши мумкин. Вақтни белгилашдан фойдаланишда сеанснинг хақиқий эканлигини тасдиқлаш учун *кечикишнинг жоиз вақт оралиги* муаммоси пайдо бўлади. Чунки, “вақт тамғаси”ли хабар, умуман, бир лахзада узатилиши мумкин эмас. Ундан ташқари, қабул қилувчи ва жўнатувчининг соатлари мутлақо синхронланган бўлиши мумкин эмас.

Аутентификация протоколларини таққослашда ва танлашда қуйидаги характеристикаларни ҳисобга олиш зарур:

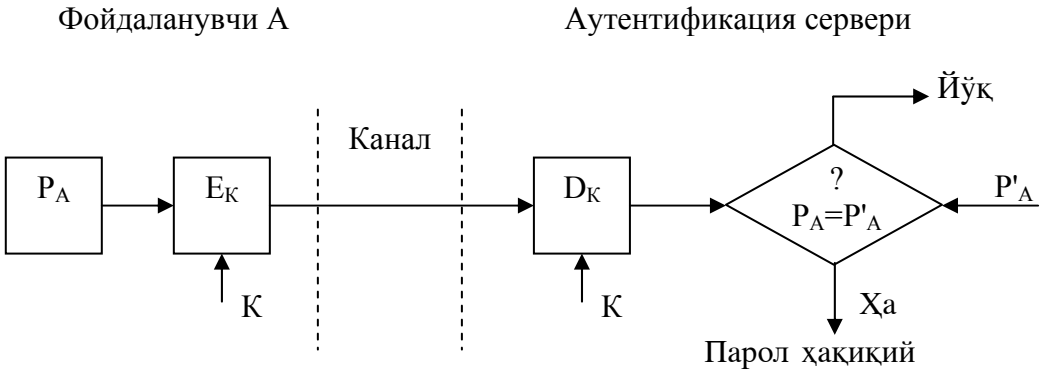
- *ўзаро аутентификациянинг мавжудлиги.* Ушбу хусусият аутентификацион алмашинув тарафлари ўртасида иккиёқлама аутентификациянинг зарурлигини акс эттиради;
- *ҳисоблаш самарадорлиги*. Протоколни бажаришда зарур бўлган амаллар сони;
- *коммуникацион самарадорлик*. Ушбу хусусият аутентификацияни бажариш учун зарур бўлган хабар сони ва узунлигини акс эттиради;
- *учинчи тарафнинг мавжудлиги*. Учинчи тарафга мисол тариқасида симметрик калитларни тақсимловчи ишончли серверни ёки очиқ калитларни тақсимлаш учун сертификатлар дарахтини амалга оширувчи серверни кўрсатиш мумкин;
- *хавфсизлик кафолати асоси.* Мисол сифатида нуллик билим билан исботлаш хусусиятига эга бўлган протоколларни кўрсатиш мумкин;
- *сирни сақлаш*. Жиддий калитли ахборотни сақлаш усули кўзда тутилади.

6.2. Пароллар асосида аутентификациялаш

Аутентификациянинг кенг тарқалган схемаларидан бири *оддий аутентификациялаш* бўлиб, у анъанавий кўп мартали паролларни ишлатиши-

га асосланган. Тармоқдаги фойдаланувчини оддий аутентификациялаш муолажасини қуйидагича тасаввур этиш мумкин. Тармоқдан фойдаланишга уринган фойдаланувчи компьютер клавиатурасида ўзининг идентификатори ва паролини теради. Бу маълумотлар аутентификация серверига ишланиш учун тушади. Аутентификация серверида сақланаётган фойдаланувчи идентификатори бўйича маълумотлар базасидан мос ёзув топилади, ундан паролни топиб фойдаланувчи киритган парол билан таққосланади. Агар улар мос келса, аутентификация муваффақиятли ўтган ҳисобланади ва фойдаланувчи легал (қонуний) мақомини ва авторизация тизими орқали унинг мақоми учун аниқланган хуқуқларни ва тармоқ ресурсларидан фойдаланишга рухсатни олади.

Паролдан фойдаланган ҳолда оддий аутентификациялаш схемаси 6.1–расмда келтирилган.



6.1-расм. Паролдан фойдаланган ҳолда оддий аутентификациялаш.

Равшанки, фойдаланувчининг паролини шифрламасдан узатиш орқали аутентификациялаш варианти хавфсизликнинг хатто минимал даражасини кафолатламайди. Паролни ҳимоялаш учун уни ҳимояланмаган канал орқали узатишдан олдин шифрлаш зарур. Бунинг учун схемага шифрлаш $E_к$ ва расшифровка қилиш $D_к$ воситалари киритилган. Бу воситалар бўлинувчи махфий калит К орқали бошқарилади. Фойдаланувчининг ҳақиқийлигини текшириш фойдаланувчи юборган парол P_A билан аутентификация серверида сақланувчи дастлабки қиймат P'_A ни таққослашга асосланган. Агар P_A ва P'_A қийматлар мос келса, парол P_A ҳақиқий, фойдаланувчи A эса қонуний ҳисобланади.

Оддий аутентификацияни ташкил этиш схемалари нафақат паролларни узатиш, балки уларни сақлаш ва текшириш турлари билан ажралиб туради. Энг кенг тарқалган усул – фойдаланувчилар паролини тизимли файлларда, очиқ ҳолда сақлаш усулидир. Бунда файлларга ўқиш ва ёзишдан ҳимоялаш атрибутлари ўрнатилади (масалан, операцион тизимдан фойдаланишни назоратлаш руйхатидаги мос имтиёзларни тавсифлаш ёрдамида). Тизим фойдаланувчи киритган паролни пароллар файлида сақланаётган ёзув билан солиштиради. Бу усулда шифрлаш ёки бир томонлама функциялар каби криптографик механизмлар ишлатилмайди. Ушбу усулнинг камчилиги – нияти бузуқ одамнинг тизимда маъмур имтиёзларидан, шу билан бирга тизим файлларидан, жумладан парол файлларидан фойдаланиш имкониятидир.

Хавфсизлик нуқтаи назаридан паролларни бир томонлама функциялардан фойдаланиб узатиш ва сақлаш қулай ҳисобланади. Бу ҳолда фойдаланувчи паролнинг очиқ шакли урнига унинг бир томонлама функция h(.) дан фойдаланиб олинган тасвирини юбориши шарт. Бу ўзгартириш ғаним томонидан паролни унинг тасвири орқали ошкор қила олмаганлигини кафолатлайди, чунки ғаним ечилмайдиган сонли масалага дуч келади.

Кўп мартали паролларга асосланган оддий аутентификациялаш тизимининг бардошлиги паст, чунки уларда аутентификацияловчи ахборот маъноли сўзларнинг нисбатан катта бўлмаган тўпламидан жамланади. Кўп мартали паролларнинг таъсир муддати ташкилотнинг хавфсизлиги сиёсатида белгиланиши ва бундай паролларни мунтазам равишда алмаштириб туриш лозим. Паролларни шундай танлаш лозимки, улар луғатда бўлмасин ва уларни топиш қийин бўлсин.

Бир мартали паролларга асосланган аутентификациялашда фойдаланишга ҳар бир сўров учун турли пароллар ишлатилади. Бир мартали динамик парол фақат тизимдан бир марта фойдаланишга яроқли. Агар, ҳатто кимдир уни ушлаб қолса ҳам парол фойда бермайди. Одатда бир мартали паролларга асосланган аутентфикациялаш тизими масофадаги фойдаланувчиларни текширишда қўлланилади.

Бир мартали паролларни генерациялаш аппарат ёки дастурий усул оқали амалга оширилиши мумкин. Бир мартали пароллар асосидаги фойдаланишнинг аппарат воситалари ташқаридан тўлов пластик карточкаларига ўхшаш микропроцессор ўрнатилган миниатюр қурилмалар кўринишда амалга оширади. Одатда калитлар деб аталувчи бундай карталар клавиатурага ва катта бўлмаган дисплей дарчасига эга.

Фойдаланувчиларни аутентификациялаш учун бир мартали паролларни қўллашнинг қуйидаги усуллари маълум:

1. Ягона вақт тизимига асосланган вақт белгилари механизмидан фойдаланиш.
2. Легал фойдаланувчи ва текширувчи учун умумий бўлган тасодифий пароллар руйхатидан ва уларнинг ишончли синхронлаш механизмидан фойдаланиш.
3. Фойдаланувчи ва текширувчи учун умумий бўлган бир хил дастлабки қийматли псевдотасодифий сонлар генераторидан фойдаланиш.

Биринчи усулни амалга ошириш мисоли сифатида SecurID аутентикациялаш технологиясини кўрсатиш мумкин. Бу технология Security Dynamics компанияси томонидан ишлаб чиқилган бўлиб, қатор компанияларнинг, хусусан Cisco Systems компаниясининг серверларида амалга оширилган.

Вақт синхронизациясидан фойдаланиб аутентификациялаш схемаси тасодифий сонларни вақтнинг маълум оралиғидан сўнг генерациялаш алгоритмига асосланган. Аутентификация схемаси қуйидаги иккита параметрдан фойдаланади:

- ҳар бир фойдаланувчига аталган ва аутентификация серверида ҳамда фойдаланувчининг аппарат калитида сақланувчи ноёб 64-битли сондан иборат махфий калит;
- жорий вақт қиймати.

Масофадаги фойдаланувчи тармоқдан фойдаланишга уринганида ундан шахсий идентификация номери PINни киритиш таклиф этилади. PIN тўртта ўнли рақамдан ва аппарат калити дисплейида акслануvчи тасодифий

соннинг олтита рақамидан иборат. Сервер фойдаланувчи томонидан киритилган PIN-коддан фойдаланиб маълумотлар базасидаги фойдаланувчининг махфий калити ва жорий вақт қиймати асосида тасодифий сонни генерациялаш алгоритмини бажаради. Сўнгра сервер генерацияланган сон билан фойдаланувчи киритган сонни таққослайди. Агар бу сонлар мос келса, сервер фойдаланувчига тизимдан фойдаланишга рухсат беради.

Аутентификациянинг бу схемасидан фойдаланишда аппарат калит ва сервернинг қатъий вақтий синхронланиши талаб этилади. Чунки аппарат калит бир неча йил ишлаши ва демак сервер ички соати билан аппарат калитининг мувофиқлиги аста-секин бузилиши мумкин.

Ушбу муаммони ҳал этишда Security Dynamics компанияси қуйидаги икки усулдан фойдаланади:

- аппарат калити ишлаб чиқилаётганида унинг таймер частотасининг меъёридан четлашиши аниқ ўлчанади. Четлашишнинг бу қиймати сервер алгоритми параметри сифатида ҳисобга олинади;
- сервер муайян аппарат калит генерациялаган кодларни кузатади ва зарурият туғилганида ушбу калитга мослашади.

Аутентификациянинг бу схемаси билан яна бир муаммо боғлиқ. Аппарат калит генерациялаган тасодифий сон катта бўлмаган вақт оралиғи мобайнида ҳақиқий парол ҳисобланади. Шу сабабли, умуман, қисқа муддатли вазият содир бўлиши мумкинки, хакер PIN-кодни ушлаб қолиши ва уни тармоқдан фойдаланишга ишлатиши мумкин. Бу вақт синхронизациясига асосланган аутентификация схемасининг энг заиф жойи ҳисобланади.

Бир мартали паролдан фойдаланувчи аутентификациялашни амалга оширувчи яна бир вариант – «сўров-жавоб» схемаси бўйича аутентификациялаш. Фойдаланувчи тармоқдан фойдаланишга уринганида сервер унга тасодифий сон кўринишидаги сўровни узатади. Фойдаланувчининг аппарат калити бу тасодифий сонни, масалан DES алгоритми ва фойдаланувчининг аппарат калити хотирасида ва сервернинг маълумотлар базасида сақланувчи махфий калити ёрдамида расшифровка қилади. Тасодифий сон - сўров шифрланган кўринишда серверга қайтарилади. Сервер ҳам ўз навбатида

ўша DES алгоритми ва сервернинг маълумотлар базасидан олинган фойдаланувчининг махфий калити ёрдамида ўзи генерациялаган тасодифий сонни шифрлайди. Сўнгра сервер шифрлаш натижасини аппарат калитидан келган сон билан таққослайди. Бу сонлар мос келганида фойдаланувчи тармоқдан фойдаланишга рухсат олади. Таъкидлаш лозимки, «сўров-жавоб» аутентификациялаш схемаси ишлатишда вақт синхронизациясидан фойдаланувчи аутентификация схемасига қараганда мураккаброқ.

Фойдаланувчини аутентификациялаш учун бир мартали паролдан фойдаланишнинг иккинчи усули фойдаланувчи ва текширувчи учун умумий бўлган тасодифий пароллар руйхатидан ва уларнинг ишончли синхронлаш механизмидан фойдаланишга асосланган. Бир мартали паролларнинг бўлинувчи рўйхати махфий пароллар кетма-кетлиги ёки тўплами бўлиб, ҳар бир парол фақат бир марта ишлатилади. Ушбу рўйхат аутентификацион алмашинув тарафлар ўртасида олдиндан тақсимланиши шарт. Ушбу усулнинг бир вариантига биноан сўров-жавоб жадвали ишлатилади. Бу жадвалда аутентификацилаш учун тарафлар томонидан ишлатилувчи сўровлар ва жавоблар мавжуд бўлиб, ҳар бир жуфт фақат бир марта ишлатилиши шарт.

Фойдаланувчини аутентификациялаш учун бир мартали паролдан фойдаланишнинг учинчи усули фойдаланувчи ва текширувчи учун умумий бўлган бир хил дастлабки қийматли псевдотасодифий сонлар генераторидан фойдаланишга асосланган. Бу усулни амалга оширишнинг қуйидаги вариантлари мавжуд:

- *ўзгартирилувчи бир мартали пароллар кетма-кетлиги.* Навбатдаги аутентификациялаш сессиясида фойдаланувчи айнан шу сессия учун олдинги сессия паролидан олинган махфий калитда шифрланган паролни яратади ва узатади;
- *бир томонлама функцияга асосланган пароллар кетма-кетлиги.* Ушбу усулнинг моҳиятини бир томонлама функциянинг кетма-кет ишлатилиши (Лампартнинг машҳур схемаси) ташкил этади. Хавфсизлик нуқтаи назаридан бу усул кетма-кет ўзгартирилувчи пароллар усулига нисбатан афзал ҳисобланади.

Кенг тарқалган бир мартали паролдан фойдаланишга асосланган аутентификациялаш протоколларидан бири Internet да стандартлаштирилган S/Key (RFC1760) протоколидир. Ушбу протокол масофадаги фойдаланувчиларнинг ҳақиқийлигини текширишни талаб этувчи кўпгина тизимларда, хусусан, Cisco компаниясининг TACACS+тизимида амалга оширилган.

Сертификатлар асосида аутентификациялаш

Тармоқдан фойдаланувчилар сони миллионлаб ўлчанганида фойдаланувчилар паролларининг тайинланиши ва сақланиши билан боғлиқ фойдаланувчиларни дастлабки руйхатга олиш муолажаси жуда катта ва амалга оширилиши қийин бўлади. Бундай шароитда рақамли сертификатлар асосидаги аутентификациялаш пароллар қўлланишига рационал альтернатива ҳисобланади.

Рақамли сертификатлар ишлатилганида компьютер тармоғи фойдаланувчилари хусусидаги ҳеч қандай ахборотни сақламайди. Бундай ахборотни фойдаланувчиларнинг ўзи сўров-сертификатларида тақдим этадилар. Бунда махфий ахборотни, хусусан махфий калитларни сақлаш вазифаси фойдаланувчиларнинг ўзига юкланади.

Фойдаланувчи шахсини тасдиқловчи рақамли сертификатлар фойдаланувчилар сўрови бўйича махсус ваколатли ташкилот-сертификация маркази CA (Certificate Authority) томонидан, маълум шартлар бажарилганида берилади. Таъкидлаш лозимки, сертификат олиш муолажасининг ўзи ҳам фойдаланувчининг ҳақиқийлигини текшириш (яъни, аутентификациялаш) босқичини ўз ичига олади. Бунда текширувчи тараф сертификацияловчи ташкилот (сертификация маркази CA) бўлади.

Сертификат олиш учун мижоз сертификация марказига шахсини тасдиқловчи маълумотни ва очиқ калитини тақдим этиши лозим. Зарурий маълумотлар руйхати олинадиган сертификат турига боғлиқ. Сертификацияловчи ташкилот фойдаланувчининг ҳақиқийлиги тасдиғини текширганидан сўнг ўзининг рақамли имзосини очиқ калит ва фойдаланувчи хусусидаги маълумот бўлган файлга жойлаштиради ҳамда ушбу очиқ калитнинг му-

айян шахсга тегишли эканлигини тасдиқлаган ҳолда фойдаланувчига сертификат беради.

Сертификат электрон шакл бўлиб, таркибида қўйидаги ахборот бўлади:

- ушбу сертификат эгасининг очиқ калити;

- сертификат эгаси хусусидаги маълумот, масалан, исми, электрон почта адреси, ишлайдиган ташкилот номи ва ҳ.;

- ушбу сертификатни берган ташкилот номи;

- сертификацияловчи ташкилотнинг электрон имзоси – ушбу ташкилотнинг махфий калити ёрдамида шифрланган сертификациядаги маълумотлар.

Сертификат фойдаланувчини тармоқ ресурсларига мурожаат этганида аутентификацияловчи восита ҳисобланади. Бунда текширувчи тараф вазифасини корпоратив тармоқнинг аутентификация сервери бажаради. Сертификатлар нафақат аутентификациялашда, балки фойдаланишнинг маълум хуқуқларини тақдим этишда ишлатилиши мумкин. Бунинг учун сертификатга қўшимча ҳошиялар киритилиб уларда сертификация эгасининг фойдаланувчиларнинг у ёки бу категориясига мансублиги кўрсатилади.

Очиқ калитларнинг сертификатлар билан узвий боғлиқлигини алоҳида таъкидлаш лозим. Сертификат нафақат шахсни, балки очиқ калит мансублигини тасдиқловчи хужжатдир. Рақамли сертификат очиқ калит ва унинг эгаси ўртасидаги мосликни ўрнатади ва кафолатлайди. Бу очиқ калитни алмаштириш хавфини бартараф этади.

Агар абонент ахборот алмашинуви бўйича шеригидан сертификат таркибидаги очиқ калитни олса, у бу сертификатдаги сертификация марказининг рақамли имзосини ушбу сертификация марказининг очиқ калити ёрдамида текшириш ва очиқ калит адреси ва бошқа маълумотлари сертификатда кўрсатилган фойдаланувчига тегишли эканлигига ишонч ҳосил қилиши мумкин. Сертификатлардан фойдаланилганда фойдаланувчилар руйхатини уларнинг пароллари билан корпорация серверларида сақлаш зарурияти йўқолади. Серверда сертификацияловчи ташкилотларнинг номлари ва очиқ калитларининг бўлиши етарли.

Сертификатларнинг ишлатилиши сертификацияловчи ташкилотларнинг нисбатан камлигига ва уларнинг очиқ калитларидан қизиққан барча шахслар ва ташкилотлар фойдалана олиши (масалан, журналлардаги нашрлар ёрдамида) тахминига асосланган.

Сертификатлар асосида аутентификациялаш жараёнини амалга оширишда сертификацияловчи ташкилот вазифасини ким бажариши хусусидаги масалани ечиш муҳим ҳисобланади. Ходимларни сертификат билан таъминлаш масаласини корхонанинг ўзи ечиши жуда табиий ҳисобланади. Корхона ўзининг ходимларини яхши билади ва улар шахсини тасдиқлаш вазифасини ўзига олиши мумкин. Бу сертификат берилишидаги дастлабки аутентификациялаш муолажасини осонлаштиради. Корхоналар сертификатларни генерациялаш, бериш ва уларга хизмат кўрсатиш жараёнларини автоматлаштиришни таъминловчи мавжуд дастурий махсулотлардан фойдаланишлари мумкин. Масалан, Netscape Communications компанияси серверларини корхоналарга шахсий сертификатларини чиқариш учун таклиф этади.

Сертификацияловчи ташкилот вазифасини бажаришда тижорат асосида сертификат бериш бўйича мустақил марказлар ҳам жалб этилиши мумкин. Бундай хизматларни, хусусан, Verisign компаниясининг сертификацияловчи маркази таклиф этади. Бу компаниянинг сертификатлари ҳалқаро стандарт X.509 талабларига жавоб беради. Бу сертификатлар маълумотлар ҳимоясининг қатор махсулотларида, жумладан ҳимояланган канал SSL протоколида ишлатилади.

6.4. Қатъий аутентификациялаш

Криптографик протоколларида амалга оширилувчи қатъий аутентификациялаш ғояси қуйидагича. Текширилувчи (исботловчи) тараф қандайдир сирни билишини намойиш этган ҳолда текширувчига ўзининг ҳақиқий эканлигини исботлайди. Масалан, бу сир аутентификацион алмашиш тарафлари ўртасида олдиндан хавфсиз усул билан тақсимланган бўлиши мумкин. Сирни билишлик исботи криптографик усул ва воситалардан фойдаланилган ҳолда сўров ва жавоб кетма-кетлиги ёрдамида амалга оширилади.

Энг муҳими, исботловчи тараф фақат сирни билишлигини намойиш этади, сирни ўзи эса аутентификацион алмашиш мобайнида очилмайди. Бу текширувчи тарафнинг турли сўровларига исботловчи тарафнинг жавоблари ёрдами билан таъминланади. Бунда якуний сўров фақат фойдаланувчи сирига ва протокол бошланишида ихтиёрий танланган катта сондан иборат бошланғич сўровга боғлиқ бўлади.

Аксарият ҳолларда қатъий аутентификациялашга биноан ҳар бир фойдаланувчи ўзининг махфий калитига эгалиги аломати бўйича аутентификацияланади. Бошқача айтганда фойдаланувчи унинг алоқа бўйича шеригининг тегишли махфий калитга эгалигини ва у бу калитни ахборот алмашинуви бўйича ҳақиқий шерик эканлигини исботлашга ишлата олиши мумкинлигини аниқлаш имкониятига эга.

X.509 стандарти тавсияларига биноан қатъий аутентификациялашнинг қуйидаги муолажалари фарқланади:

- бир томонлама аутентификация;
- икки томонлама аутентификация;
- уч томонлама аутентификация.

Бир томонлама аутентификациялаш бир томонга йўналтирилган ахборот алмашинувини кўзда тутади. Аутентификациянинг бу тури қуйидагиларга имкон яратади:

- ахборот алмашинувчининг фақат бир тарафини ҳақиқийлигини тасдиқлаш;
- узатилаётган ахборот яхлитлигининг бузилишини аниқлаш;
- "узатишнинг такрори" типидаги хужумни аниқлаш;
- узатилаётган аутентификацион маълумотлардан фақат текширувчи тараф фойдаланишини кафолатлаш.

Икки томонлама аутентификацилашда бир томонлилигига нисбатан исботловчи тарафга текширувчи тарафнинг қўшимча жавоби бўлади. Бу жавоб текширувчи томонни алоқанинг айнан аутентификация маълумотлари мўлжалланган тараф билан ўрнатилаётганига ишонтириш лозим.

Уч томонлама аутентификациялаш таркибида исботловчи тарафдан текширувчи тарафга қўшимча маълумотлар узатиш мавжуд. Бундай ён-

дашиш аутентификация ўтказишда вақт белгиларидан фойдаланишдан воз кечишга имкон беради.

Таъкидлаш лозимки, ушбу туркумлаш шартлидир. Амалда ишлатилувчи усул ва воситалар тўплами аутентификация жараёнини амалга оширишдаги муайян шарт-шароитларга боғлиқ. Қатъий аутентификациянинг ўтказилиши ишлатиладиган криптографик алгоритмлар ва қатор қўшимча параметрларни тарафлар томонидан сўзсиз мувофиқлаштиришни талаб этади.

Қатъий аутентификациялашнинг муайян вариантларини кўришдан олдин бир мартали параметрларнинг вазифалари ва имкониятларига тўхташ лозим. Бир мартали параметрлар баъзида "nonces" – бир мақсадга бир мартадан ортиқ ишлатилмайдиган катталик деб аталади.

Ҳозирда ишлатиладиган бир мартали параметрлардан тасодифий сонлар, вақт белгилари ва кетма-кетликларнинг номерларини кўрсатиш мумкин.

Бир мартали параметрлар узатишнинг такрорланишини, аутентификацион алмашинув тарафларини алмаштириб қўйишни ва очиқ матнни танлаш билан хужум қилишни олдини олишга имкон беради. Бир мартали параметрлар ёрдамида узатиладиган хабарларнинг ноёблигини, бир маънолилигини ва вақтий кафолатларини таъминлаш мумкин. Бир мартали параметрларнинг турли хиллари алоҳида ишлатилиши, ёки бир-бирини тўлдириши мумкин.

Бир мартали параметрларнинг қуйидаги ишлатилиш мисолларини кўрсатиш мумкин:

- "сўров-жавоб" принципида қурилган протоколларда ўз вақтидалигини текшириш. Бундай текширишда тасодифий сонлар, соатларни синхронлаш билан вақт белгилари ёки муайян жуфт (текширувчи, исботловчи) учун кетма-кетликларнинг номерларидан фойдаланиш мумкин;

- ўз вақтидалигини ёки ноёблик кафолатини таъминлаш. Протоколнинг бир мартали параметрларини бевосита (тасодифий сонни танлаш йўли билан) ёки билвосита (бўлинувчи сирдаги ахборотни тахлиллаш ёрдамида) назоратлаш орқали амалга оширилади;

- хабарни ёки хабарлар кетма-кетлигини бир маъноли идентификациялаш. Бир оҳангда ўсувчи кетма-кетликнинг бир мартали қийматини (масалан, серия номерлари ёки вақт белгилари кетма-кетлиги) ёки мос узунликдаги тасодифий сонларни тузиш орқали амалга оширилади.

Таъкидлаш лозимки, бир мартали параметрлар криптографик протоколларнинг бошқа вариантларида ҳам (масалан, калит ахборотини тақсимлаш протоколларида) кенг қўлланилади.

Қатъий аутентификациялаш протоколларини қўлланиладиган криптографик алгоритмларига боғлиқ ҳолда қуйидаги гуруҳларга ажратиш мумкин:

- шифрлашнинг симметрик алгоритмлари асосидаги қатъий аутентификациялаш протоколлари;

- бир томонлама калитли хеш-функциялар асосидаги қатъий аутентификациялаш протоколлари;

- шифрлашнинг асимметрик алгоритмлари асосидаги қатъий аутентификациялаш алгоритмлари;

- электрон рақамли имзо асосидаги қатъий аутентификациялаш алгоритмлари.

Симметрик алгоритмларга асосланган қатъий аутентификациялаш. Kerberos протоколи.

Симметрик алгоритмлар асосида қурилган аутентификациялашнинг ишлаши учун текширувчи ва исботловчи айни бошидан битта махфий калитга эга бўлишлари зарур. Фойдаланувчилари кўп бўлмаган ёпиқ тизимлар учун фойдаланувчиларнинг ҳар бир жуфти махфий калитни ўзаро бўлиб олишлари мумкин. Симметрик шифрлаш технологиясини қўлловчи катта тақсимланган тизимларда ишончли сервер қатнашувидаги аутентификациялаш протоколларидан фойдаланилади. Бу сервер билан ҳар бир тараф калитни билишлигини ўртоқлашишади.

Ушбу ёндашиш содда бўлиб туюлсада, аслида бундай аутентификациялаш протоколини ишлаб чиқиш мураккаб ва хавфсизлик нуқтаи назаридан шубхасиз эмас.

Қуйида шифрлашнинг симметрик алгоритмларига асосланган, ISO/IEC9798-2да спецификацияланган аутентификациялаш протоколлари-

нинг учта мисоли келтирилган. Бу протоколлар бўлинувчи махфий калитларни олдиндан тақсимланишини кўзда тутади. Аутентфикациялашнинг қуйидаги вариантларини кўриб чиқамиз.

- вақт белгиларидан фойдаланувчи бир томонлама аутентификациялаш.

- тасодифий сонлардан фойдаланувчи бир томонлама аутентификациялаш.

- икки томонлама аутентификациялаш.

Бу вариантларнинг ҳар бирида фойдаланувчи махфий калитни билишини намойиш қилган ҳолда, ўзининг ҳақиқийлигини исботлайди, чунки ушбу махфий калит ёрдамида сўровларни расшифровка қилади. Аутентификациялаш жараёнида симметрик шифрлашни қўллашда узатиладиган маълумотларнинг яхлитлигини таъминлаш механизмини расм бўлиб қолган усуллар асосида амалга ошириш ҳам зарур.

Қуйидаги белгилашларни киритамиз:

$г_A$- қатнашувчи А генерациялаган тасодифий сон;

$г_B$- қатнашувчи В генерациялаган тасодифий сон;

t_A- қатнашувчи А генерациялаган вақт белгиси;

E_K- калит Кда симметрик шифрлаш (калит К олдиндан А ва В ўртасида тақсимланиши шарт).

Вақт белгиларига асосланган бир томонлама аутентификациялаш:

$A \rightarrow B: E_K (t_A, B)$ (1)

Ушбу хабарни олиб расшифровка қилганидан сўнг қатнашувчи В вақт меткаси t_A ҳақиқий эканлигига ва хабарда кўрсатилган идентификатор ўзиники билан мос келишига ишонч ҳосил қилади. Ушбу хабарни қайтадан узатишни олдини олиш калитни билмасдан туриб вақт меткаси t_A ни ва индентификатор Вни ўзгартириш мумкин эмаслигига асосланади.

Тасодифий сонлардан фойдаланишга асосланган бир томонлама аутентфикациялаш:

$A \leftarrow B : r_B$ (1)

$A \rightarrow B : E_K(r_B, B)$ (2)

Қатнашувчи B қатнашувчи A га тасодифий сон r_B ни жўнатади. Қатнашувчи A олинган сон r_B ва идентификатор B дан иборат хабарни шифрлайди ва шифрланган хабарни қатнашувчи B га жўнатади. Қатнашувчи B олинган хабарни расшифровка қилади ва хабардаги тасодифий сонни қатнашувчи Ага юборгани билан таққослайди. Қўшимча у хабардаги исмни текширади.

Тасодифий қийматлардан фойдаланувчи икки томонлама аутентификациялаш:

$$A \leftarrow B : r_B \qquad (1)$$

$$A \rightarrow B : E_K(r_A, r_B, B) \qquad (2)$$

$$A \leftarrow B : E_K(r_A, r_B) \qquad (3)$$

Иккинчи ахборотни олиши билан қатнашувчи B олдинги протоколдаги текширишни амалга оширади ва қатнашувчи A га аталган учунчи хабарга киритиш учун қўшимча тасодифий сон r_A ни расшифровка қилади. Қатнашувчи A учинчи хабарни олганидан сўнг r_A ва r_B ларнинг қийматларини текшириш асосида айнан қатнашувчи B билан ишлаётганига ишонч ҳосил қилади.

Аутентификация жараёнида учинчи тарафни жалб этиш билан фойдаланувчиларни аутентификациялашни таъминловчи протоколларнинг машҳур намуналари сифатида Нидхэм ва Шредернинг махфий калитларни тақсимлаш протоколини ва Kerberos протоколини кўрсатиш мумкин.

Kerberos протоколи "мижоз-сервер" ва ҳам локал ва ҳам глобал тармоқларда ишловчи абонентлар орасида алоқанинг ҳимояланган каналини ўрнатишга аталган калит ахборотини алмашиш тизимларида аутентификациялаш учун ишлатилади. Бу протоколнинг Microsoft Windows 2000 ва UNIX BSD операцион тизимларига аутентификациялашнинг асосий протоколи сифатида ўрнатилганлиги алоҳида қизиқиш ўйғотади.

Kerberos ишонч қозонмаган тармоқларда аутентификациялашни таъминлайди, яъни Kerberos ишлашида нияти бузуқ одамлар қуйидаги ҳаракатларни бажаришлари мумкин:

- ўзини тармоқ уланишининг эътироф этилган тарафларидан бири деб кўрсатиш;

- уланишда иштирок этаётган компьютерларнинг биридан фойдалана олиш;

- ҳар қандай пакетни ушлаб қолиш, уларни модификациялаш ва/ёки иккинчи марта узатиш.

Kerberos протоколида хавфсизлик таъминоти юқорида келтирилган нияти бузуқ одамларнинг харакатлари натижасида пайдо бўладиган ҳар қандай муаммоларнинг бартарафланишини таъминлайди.

Kerberos протоколи олдинги асрнинг 80-йилларида яратилган ва шу пайтгача бешта версияда ўз аксини топган қатор жиддий ўзгаришларга дучор бўлди.

Kerberos TCP/IP тармоқлари учун яратилган бўлиб, протокол қатнашчиларининг учинчи(ишонилган) тарафга ишонишлари асосига қурилган. Тармоқда ишловчи Kerberos хизмати ишонилган воситачи сифатида ҳаракат қилиб, тармоқ ресурсларидан мижознинг (мижоз иловасининг) фойдалинишини авторизациялаш билан тармоқда ишончли аутентификациялашни таъминлайди. Kerberos хизмати алоҳида махфий калитни тармоқнинг ҳар бир субъекти билан бўлишади ва бундай махфий калитни билиш тармоқ субъекти ҳақиқийлигининг исботига тенг кучлидир.

Kerberos асосини Нидхем-Шредернинг учинчи ишонилган тараф билан аутентификациялаш ва калитларни тақсимлаш протоколи ташкил этади. Нидхем-Шредер протоколининг ушбу версиясини Kerberosга татбиқан кўрайлик. Kerberos протоколида (5-версия) алоқа қилувчи иккита тараф ва калитларни тақсимлаш маркази KDC(Key Distribution Center) вазифасини бажарувчи ишонилган сервер KS иштирок этади.

Чақирувчи объект А орқали, чақирилувчи объект В орқали белгиланади. Сеанс қатнашчилари, мос ҳолда Id_A ва Id_B ноёб идентификаторларга эга. А ва В тарафлар, ҳар бири алоҳида, ўзининг махфий калитини сервер KS билан бўлишади.

Айтайлик, А тараф В тараф билан ахборот алмашиш мақсадида сеанс калитини олмоқчи. А тараф тармоқ орқали сервер KSга Id_A ва Id_B идентификаторларни юбориш билан калитлар тақсимланиши даврини бошлаб беради:

$$A \to KS : Id_A, Id_B$$

Сервер KS вақтий белги T, таъсир муддати L, тасодифий калит K ва идентфикатор Id_A бўлган хабарни генерациялаб, бу хабарни B тараф билан бўлинган махфий калит ёрдамида шифрлайди.

Сўнгра сервер KS B тарафга тегишли вақтий белги T, таъсир муддати L, тасодифий калит K, идентификатор Id_B ни олиб уни A тараф билан бўлинган махфий калит ёрдамида шифрлайди. Бу иккала шифрланган хабарларни A тарафга жўнатади.

$$KS \to A : E_A(T, L, K, Id_B), E_B(T, L, K, Id_A)$$

A тараф биринчи хабарни ўзининг махфий калити билан расшифровка қилади ва ушбу хабар калитлар тақсимотининг олдинги муолажасининг қайтарилиши эмаслигига ишонч ҳосил қилиш мақсадида вақт белгиси T ни текширади. Сўнгра A тараф ўзининг идентификатори Id_A ва вақт белгиси билан хабарни генерациялаб, уни сеанс калити K ёрдамида шифрлайди ва B тарафга узатади. Ундан ташқари, A тараф B тараф учун KS дан B тараф калити ёрдамида шифрланган хабарни жўнатади:

$$A \to B : E_K(Id_A, T), E_B(T, L, K, Id_A)$$

Бу хабарни фақат B тараф расшифровака қилиши мумкин. B тараф вақт белгиси T, таъсир муддати L, сеанс калити K ва идентификатор Id_A ни олади. Сўнгра B тараф сеанс калит K ёрдамида хабарнинг иккинчи қисмини расшифровка қилади. Хабарнинг иккала қисмидаги T ва Id_A қийматларининг мос келиши A нинг B га нисбатан ҳақиқийлигини тасдиқлайди.

Хақиқийликни ўзаро тасдиқлаш мақсадида B тараф вақт белгиси T плюс 1 дан иборат хабар яратади, уни K калит ёрдамида шифрлайди ва A тарафга жўнатади.

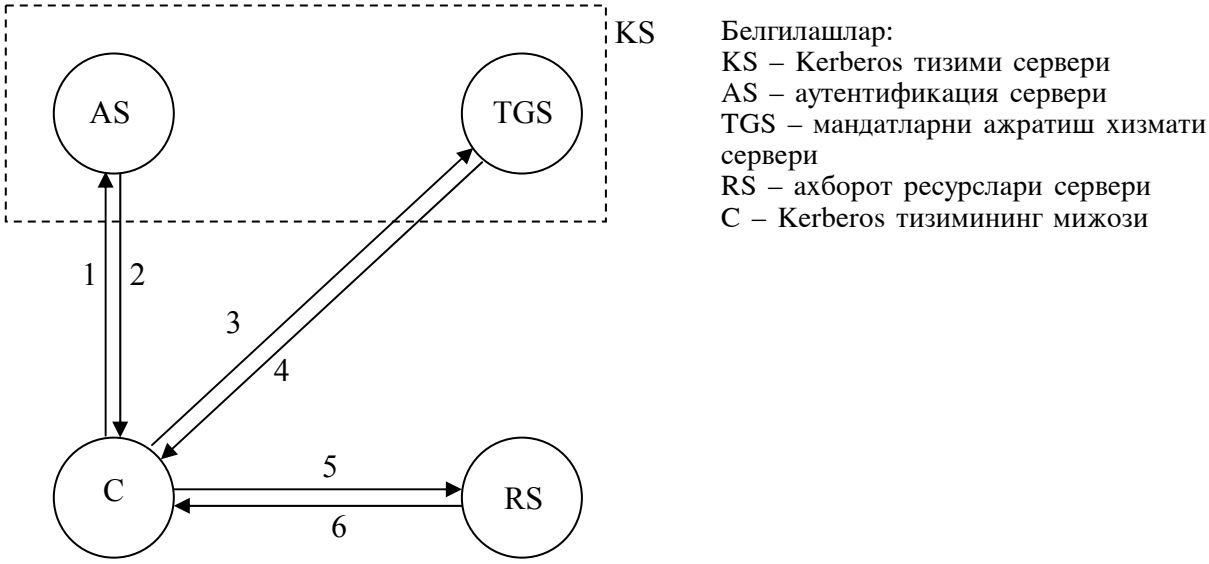
$$B \to A : E_K(T + 1)$$

Агар бу хабар (4) расшифровка қилингандан кейин A тараф кутилган натижани олса, у алоқа линиясининг бошқа тарафида ҳақиқатан B турганлигига ишонч ҳосил қилади.

Бу протокол барча қатнашувчиларнинг соатлари сервер KS соатлари билан синхронланганида муваффақиятли ишлайди. Таъкидлаш лозимки, бу

протоколда *A* тарафнинг *B* тараф билан алоқа ўрнатишга ҳар бир хоҳишида сеанс калитини олиш учун KS билан алмашинув зарур бўлади. Протоколнинг *A* ва *B* объектларни ишончли улаши учун, ҳеч бир калит обрўсизланмаслиги ва сервер KS нинг ҳимояланиши талаб этилади.

Умуман *Kerberos* тизимида (5 версия) фойдаланувчини идентификациялаш ва аутентификациялаш жараёнини қуйидагича тавсифлаш мумкин (6.2-расм).



6.2-расм. Kerberos протоколининг ишлаш схемаси

Мижоз *C*, тармоқ ресурсидан фойдаланиш мақсадида аутентификация сервери *AS* га сўров йўллайди. Сервер *AS* фойдаланувчини унинг исми ва пароли ёрдамида идентификациялайди ва мижозга мандат ажратиш хизмати сервери *TGS*дан (*Ticket Grating Service*) фойдаланишга мандат юборади.

Ахборот ресурсларининг муайян мақсадли сервери *RS* дан фойдаланиш учун мижоз *C TGS* дан мақсадли сервер *RS* га мурожаат қилишга мандат сўрайди. Ҳамма нарса тартибда бўлса *TGS* керакли тармоқ ресурсларидан фойдаланишга рухсат бериб, клиент *C* га мос мандатни юборади.

Kerberos тизими ишлашининг асосий қадамлари (6.2.-расмга қаралсин):

1. $C \rightarrow AS$ - мижоз *C* нинг *TGS* хизматига мурожаат қилишга рухсат сўраб сервер *AS*дан сўрови.

2. $AS \rightarrow C$ - сервер *AS* нинг мижоз *C* га *TGS* хизматидан фойдаланишга рухсати (мандати).

3. $C \to TGS$ - мижоз *C* нинг ресурслар сервери *RS* дан фойдаланишга рухсат (мандат) сўраб, *TGS* хизматидан сўрови.

4. $TGS \to C$ - *TGS* хизматининг мижоз *C* га ресурслар сервери *RS* дан фойдаланишига рухсати (мандати).

5. $C \to RS$ - сервер *RS* дан ахборот ресурсининг (хизматнинг) сўрови.

6. $RS \to C$ - сервер *RS* нинг хақиқийлигини тасдиқлаш ва мижоз *C* га ахборот ресурсини (хизматни) тақдим этиш.

Мижоз билан сервер алоқасининг ушбу модели фақат узатиладиган бошқарувчи ахборотнинг конфиденциаллиги ва яхлитлиги таъминланганида ишлаши мумкин. Ахборот хавфсизлигини қатъий таъминламасдан *AS, TGS* ва *RS* серверларга мижоз *C* сўров юбораолмайди ва тармоқ хизматидан фойдаланишга рухсат ололмайди.

Ахборотнинг ушлаб қолиниши ва рухсатсиз фойдаланиши имкониятларини бартараф этиш мақсадида Kerberos тармоқда ҳарқандай бошқариш ахбороти узатилганида махфий калитлар комплексини (мижознинг махфий калити, сервернинг махфий калити, мижоз-сервер жуфтининг махфий сеанс калитлари) кўп марта шифрлашни ишлатади. Kerberos шифрлашнинг турли алгоритмларидан ва хэш-функциялардан фойдаланиши мумкин, аммо мададлаш учун Triple DES ва MD5 алгоритмлари ўрнатилган.

Kerberos тизимида ишонч хужжатларининг икки туридан фойдаланилади: мандат (tricket) ва аутентификатор (authentifacator).

Мандат серверга мандат берилган мижознинг идентификацион маълумотларини хавфсиз узатиш учун ишлатилади. Унинг таркибида ахборот ҳам бўлиб, ундан сервер мандатдан фойдаланаётган мижознинг хақиқий эканлигини текширишда фойдаланиши мумкин.

Аутентификатор – мандат билан бирга кўрсатилувчи қўшимча атрибут(аломат). Қуйида Kerberos хужжатларида ишлатилувчи белгилашлар тизими келтирилган:

C – мижоз;

S – сервер;

a – мижознинг тармоқ адреси;

v – мандат таъсири вақтининг бошланиши ва охири;

T – вақт белгиси;

K_x – махфий калит x;

K_{xy} – x ва y учун сеанс калити;

$\{m\}K_x$ – субъект x нинг махфий калити K_x билан шифрланган хабар m;

$T_{x,y}$ – y дан фойдаланишга мандат x;

$A_{x,y}$ – x ва y учун аутентификатор.

Kerberos мандати.

Kerberos мандати қуйидаги шаклга эга: $T_{c,s} = S, \{C, a, v, K_{C,S}\}K_S$.

Мандат битта мижозга қатъий белгиланган сервердан фойдаланиш учун қатъий белгиланган вақтга берилади. Унинг таркибида мижоз исми, унинг тармоқ адреси, мижоз ҳаракатининг бошланиш ва тугаш вақти ва сервернинг махфий калити K_S шифрланган сеанс калити $K_{C,S}$ бўлади. Мижоз мандатни расшифровка қилаолмайди (у сервернинг махфий калитини билмайди), аммо у мандатни шифрланган шаклда серверга кўрсатиши мумкин. Мандат тармоқ орқали узатилаётганда тармоқдаги яширинча эшитиб турувчиларнинг бирортаси ҳам уни ўқий олмайди ва ўзгартира олмайди.

Kerberos аутентификатори.

Kerberos аутентификатори қуйидаги шаклга эга: $A_{C,S} = \{C, t, калит\}K_{C,S}$

Мижоз мақсадли сервердан фойдаланишни хоҳлаганида аутентификаторни яратади. Унинг таркибида мижоз исми, вақт белгиси, мижоз ва сервер учун умумий бўлган сеанс калити $K_{C,S}$ шифрланган сеанс калити бўлади. Мандатдан фарқли ҳолда аутентификатор бир марта ишлатилади.

Аутентификаторнинг ишлатилиши иккита мақсадни кўзлайди. Биринчидан, аутентификаторда сеанс калитида шифрланган қандайдир матн бўлади. Бу калитнинг мижозга маълумлигидан далолат беради. Иккинчидан, шифрланган очиқ матнда вақт белгиси мавжуд. Бу вақт белгиси аутентификатор ва мандатни ушлаб қолган нияти бузуқ одамга улардан бирор вақт ўтганидан сўнг аутентфикациялаш муолжасини ўтишда ишлатишига имкон бермайди.

Kerberos хабарлари.

Kerberosнинг 5-версиясида хабарларнинг қуйидаги турлари ишлатилади (6.3-расмга қаралсин).

1. Мижоз – Kerberos: *C, tgs.*
2. Kerberos – мижоз : $\{K_{c,tgs}\}K_c\{T_{cftgs}\}K_{tgs}$.
3. Мижоз – $TGS:\{A_C,_S\}K_{C,tgs}(T_{C,tgs})K_{tgs,S}$.
4. TGS – мижоз: $\{K_{C,S}\}K_{C,tgs}\{T_{C,S}\}K_S$,.
5. Мижоз – сервер: $\{A_{C,S}\}K_{C,S}\{T_{C,S}\}K_S$.

Ушбу хабарлардан фойдаланишни батафсил кўрайлик.

Дастлабки мандатни олиш.

Мижоздан шахсини исботловчи ахборотнинг қисми – унинг пароли мавжуд. Мижозни паролини тармоқ орқали жўнатишига мажбур қилиб бўлмайди. Kerberos протоколи паролни обрўсизлантириш эҳтимолини минималлаштиради, аммо агар фойдаланувчи паролни билмаса унга ўзини тўғри идентификациялашга имкон бермайди.

Мижоз Kerberosнинг аутентификация серверига ўзининг исми, сервери *TGS* нинг (бир нечта сервер *TGS* бўлиши мумкин) бўлган хабарни жўнатади. Амалда фойдаланувчи кўпинча исмини ўзини киритади, тизимга кириш дастури эса сўров юборади.

Kerberosнинг аутентификациялаш сервери ўзининг маълумотлар базасида мижоз хусусидаги маълумотларни қидиради. Агар мижоз хусусидаги ахборот маълумотлар базасида бўлса, Kerberos мижоз ва *TGS* орасида маълумот алмашиш учун ишлатиладиган сеанс калитини генерациялайди. Kerberos бу сеанс калитини мижознинг махфий калити билан шифрлайди. Сўнгра у *TGS* хизматига мижознинг хақиқийлигини исботловчи *TGT* (*Ticket Granting Ticket*) мандатининг ажратилиши учун мижозга мандат яратади. *TGS* нинг махфий калитида *TGT* шифрланади ва унинг таркибида мижоз ва сервер идентификатори, *TGS* – мижоз жуфтининг сеанс калити, ҳамда *TGT* таъсирининг бошланиш ва охирги вақтлари бўлади. Аутентификациялаш сервери бу иккита шифрланган хабарни мижозга юборади.

Энди мижоз бу хабарларни қабул қилади, биринчи хабарни ўзининг махфий калити K_C билан расшифровка қилиб, сеанс калити $K_{C,tgs}$ ни ҳосил қилади. Махфий калит мижоз паролининг бир томонлама хэш-функцияси

бўлганлиги сабабли қонуний фойдаланувчида ҳеч қандай муаммо туғилмайди. Нияти бузуқ одам тўғри паролни билмайди ва, демак, аутентификациялаш серверининг жавобини расшифровка қила олмайди. Шу сабабли нияти бузуқ одам мандатни ёки сеанс калитини ола олмайди. Мижоз *TGT* мандатини ва сеанс калитини сақлаб, парол ва хэш-қийматни, уларнинг обрўсизланиш эҳтимолликларини пасайтириш мақсадида, ўчиради. Агар нияти бузуқ одам мижоз хотираси таркибининг нусхасини олишга ўринса, у фақат *TGT* ва сеанс калитини олади. Бу маълумотлар фақат *TGT* таъсири вақтидагина муҳим ҳисобланади. *TGT* таъсир муддати тугагунидан сўнг бу маълумотлар маънога эга бўлмайди. Энди мижоз *TGT* дан олинган мандат ёрдамида унда кўрсатилган *TGT* таъсирининг бутун муддати мобайнида сервер *TGS* да аутентификациялашдан ўтиш имкониятига эга.

Сервер мандатларини олиш.

Мижоз ўзига керак бўлган ҳар бир хизмат учун алоҳида мандат олиши мумкин. Шу мақсадда мижоз *TGS* хизматига *TGT* мандати ва аутентификатордан иборат сўров юбориши лозим. (Амалда сўровни дастурий таъминот автоматик тарзда, яъни фойдаланувчига билдирмасдан юборади.) Мижоз ва *TGS* сервери жуфтининг калитида шифрланган аутентификатор таркибида мижоз ва унга керакли сервернинг идентификатори, тасодифий сеанс калити ва вақт белгиси бўлади.

TGS сўровни олиб, ўзининг махфий калитида *TGT* ни расшифровка қилади. Сўнгра *TGS TGT* даги сеанс калитидан аутентификаторни расшифровка қилишда фойдаланади. Ниҳоясида аутентификатордаги ахборотни мандат ахбороти билан таққосланади. Аниқроғи, билетдаги мижознинг тармоқ адреси сўровда кўрсатилган тармоқ адреси билан, ҳамда вақт белгиси жорий вақт билан солиштирилади. Агар барчаси мос келса, *TGS* сўровни бажаришга рухсат беради.

Вақт белгиларини текширишда барча компьютерларнинг соатлари, бўлмаганда, бир неча минут аниқлигида синхронланганлиги кўзда тутилади. Агар сўровда кўрсатилган вақт жорий ондан анчагина фарқ қилса, TGS бундай сўровни олдинги сўровни қайтаришга уриниш деб ҳисоблайди.

TGS хизмати аутентификатор таъсири муддатининг тўғрилигини кузатилиши лозим, чунки сервер хизмати битта мандат, аммо турли аутентификаторлар ёрдамида кетма-кет бир неча марта сўралиши мумкин. Ўша мандат ва аутентификаторнинг ишлатилган вақт белгиси билан қилинган сўров қайтарилади.

Тўғри сўровга жавоб тариқасида *TGS* мижозга мақсад сервердан фойдаланиш учун мандат тақдим этади. *TGS* мижоз ва мақсад сервери учун мижоз ва *TGS* га умумий бўлган сеанс калитида шифрланган сеанс калитини ҳам яратади. Бу иккала хабар мижозга юборилади. Мижоз хабарни расшифровка қилади ва сеанс калитини чиқариб олади.

Хизмат сўрови.

Энди мижоз ўзининг ҳақиқийлигини мақсад серверига исботлаши мумкин. Мақсад серверида аутентификациядан муваффақиятли ўтиш учун мижоз таркибида ўзининг исми, тармоқ адреси, вақт белгиси бўлган ва сеанс калити "мижоз-сервер"да шифрланган аутентификаторни яратади ва уни TGS хизматидан олиб берилган мақсад серверининг махфий калитида шифрланган мандат билан бирга жўнатади.

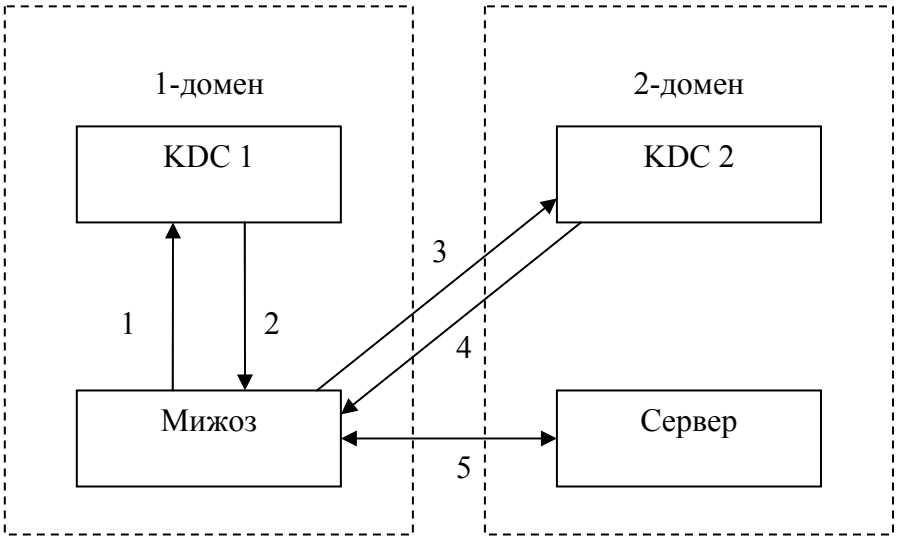
Мақсад сервери мижоздан маълумотларни олиб, аутентификаторни ўзининг махфий калитида расшифровка қилади ва ундан "мижоз-сервер" сеанс калитини чиқариб олади. Мандат ҳам текширилади. Текшириш муолажаси "мижоз-TGS" сессиясида ўтказиладиган муолажага ўхшаш, яъни тармоқ адреслари ва вақт белгисининг мослиги текширилади. Агар барчаси мос келса, сервер мижознинг хақиқийлигига ишонч ҳосил қилади.

Агар илова ҳақиқийликнинг ўзаро текширилишини талаб этса, сервер мижозга таркибида сеанс калитида шифрланган вақт белгиси бўлган хабарни юборади. Бу серверга тўғри махфий калитнинг маълум эканлигини ва у мандат ва гувоҳномани расшифровка қила олишини исботлайди. Зарурият туғилганида мижоз ва сервер кейинги хабарларни умумий калитда шифрлашлари мумкин. Чунки бу калит фақат уларга маълум, бу калит билан шифрланган охирги хабар иккинчи тарафдан юборилганига иккала тараф ишонч ҳосил қилишлари мумкин. Амалда бу барча мураккаб муолажалар

автоматик тарзда бажарилади ва мижозга қандайдир ноқулайликлар етказилмайди.

Доменлараро аутентификациялаш хусусиятлари.

Kerberos дан доменлараро аутентификациялашда ҳам фойдаланиш мумкин. Мижоз бошқа домендаги сервердан фойдаланиш мақсадида калитларни тақсимлаш маркази *KDC* га мурожаат қилса, *KDC* мижозга суралаётган сервер жойлашган доменнинг *KDC* ига мурожаат этишга *қайта адреслаш мандатини* (referal ticket) тақдим этади (6.4-расм).



6.4-расм. Kerberos протоколида доменлараро аутентификациялаш схемаси

Расмда қуйидаги белгилашлар қабул қилинган:

1. Аутентификациялашга сўров.
2. *KDC*1 учун *TGT*
3. *KDC*2 учун *TGT*.
4. Сервердан фойдаланиш мандати.
5. Маълумотларни аутентификациялаш ва алмашиш.

Қайта адреслаш мандати иккита домен KDCсининг жуфтли алоқа калитида шифрланган TGTдир. Бунда мижозга сервердан фойдаланишга мандатни сўралаётган сервер жойлашган KDC тақдим этади.

Жуда кўп доменли тармоқда аутентификациялаш учун Kerberosдан фойдаланиш назарий жиҳатдан мумкин бўлсада, мурожаатлар сонининг доменлар сонига мутаносиб равишда ошиши сабабли, сўровларни муайян

KDCларга бир маънода қайта адресловчи қандайдир марказий домен қуришга тўғри келади.

Kerberos хавфсизлиги.

Kerberos, криптографик ҳимоялашнинг бошқа ҳарқандай дастурий воситаси каби ишончсиз дастурий муҳитда ишлайди. Ушбу муҳитнинг хужжатлаштирилмаган имкониятлари ёки нотўғри конфигурацияси жиддий ахборотнинг чиқиб кетишига олиб келиши мумкин. Хатто калитлар фойдаланувчи ишлаш сеансида фақат оператив хотирада сақланса ҳам операцион тизимдаги бузилиш калитларнинг қаттиқ дискда нусхаланишига олиб келиши мумкин.

Kerberos дастурий таъминоти ўрнатилган ишчи станциясидан кўпчилик фойдаланувчи режимнинг ишлатилиши ёки ишчи станциялардан фойдаланишнинг назорати бўлмаслиги дастур-закладкани киритиш ёки криптографик дастурий таъминотни модификациялаш имкониятини туғдиради.

Шу сабабли, Kerberos хавфсизлиги кўп жиҳатдан ушбу протокол ўрнатилган ишчи станцияси ҳимоясининг ишончлигига боғлиқ.

Kerberos протоколининг ўзига қуйидаги қатор талаблар қуйилади:

- Kerberos хизмати хизмат қилишдан воз кечишга йўналтирилган хужумлардан ҳимояланиши шарт;

- вақт белгиси аутентификация жараёнида қатнашиши сабабли, тизимдан фойдаланувчиларининг барчаси учун тизимли вақтни синхронлаш зарур;

- Kerberos паролни саралаш орқали хужум қилишдан ҳимояламайди. Муаммо шундаки, *KDC* да сақланувчи фойдаланувчи калити унинг паролини хэш-функция ёрдамида қайта ишлаш натижасидир. Паролнинг бўшлигида уни саралаб топиш мумкин.

- Kerberos хизмати рухсатсиз фойдаланишининг барча турларидан ишончли ҳимояланиши шарт;

- мижоз олган мандатлар, ҳамда махфий калитлар рухсатсиз фойдаланишдан ҳимояланиши шарт.

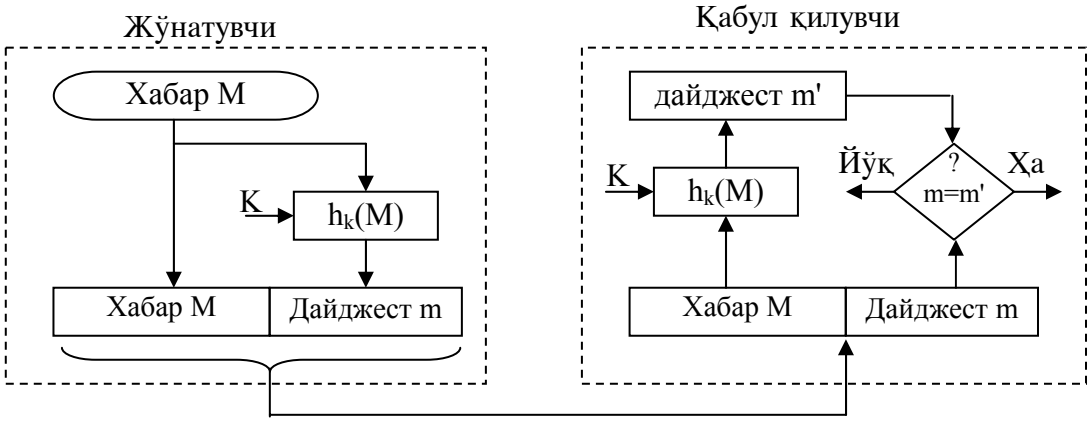
Юқорида келтирилган талабларнинг бажарилмаслиги муваффақиятли хужумга сабаб бўлиши мумкин.

Ҳозирда Kerberos протоколи аутентификациялашнинг кенг тарқалган воситаси ҳисобланади. Kerberos турли криптографик схемалар, хусусан, очиқ калитли шифрлаш билан биргаликда ишлатилиши мумкин.

Бир томонлама калитли хэш-функциялардан фойдаланишга асосланган протоколлар.

Бир томонлама хэш-функция ёрдамида шифрлашнинг ўзига хос хусусияти шундаки, у моҳияти бўйича бир томонламадир, яъни тескари ўзгартириш-қабул қилувчи тарафда расшифровка қилиш билан бирга олиб борилмайди. Иккала тараф (жўнатувчи ва қабул қилувчи) бир томонлама шифрлаш муолажасидан фойдаланади.

Шифрланаётган маълумот *M* га қўлланилган *K* параметр-калитли бир томонлама хэш-функция $h_k(.)$ натижада байтларнинг белгиланган катта бўлмагани сонидан иборат хэш-қиймат (дайджест) "*m*" ни беради (6.4-расм).



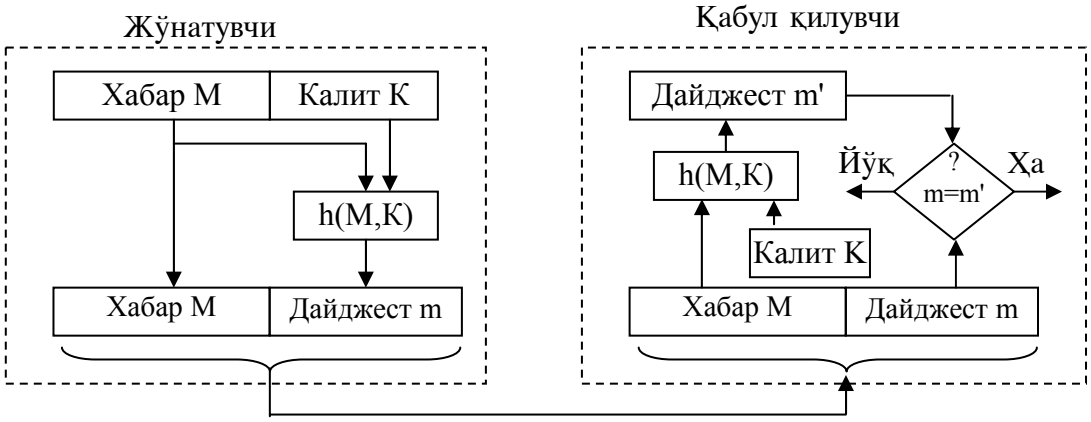
6.4–расм. Маълумотлар яхлитлигини текширишда бир томонлама хэш-функциянинг ишлатилиши (I-вариант).

Дайджест "m" қабул қилувчига дастлабки хабар *M* билан бирга узатилади. Хабарни қабул қилувчи, дайджест олинишида қандай бир томонлама хэш-функция ишлатилганлигини билган ҳолда, расшифровка қилинган хабар *M* дан фойдаланиб, дайджестни бошқатдан ҳисоблайди. Агар олинган дайджест билан ҳисобланган дайджест мос келса, хабар *M* нинг таркиби ҳеч қандай ўзгаришга дучор бўлмаганини билдиради.

Дайджестни билиш дастлабки хабарни тиклашга имкон бермайди, аммо маълумотлар яхлитлигини текширишга имкон беради. Дайджестга дастлабки хабар учун ўзига хос назорат йиғиндиси сифатида қараш мумкин. Аммо, дайджест ва оддий назорат йиғиндиси орасида жиддий фарқ ҳам мавжуд. Назорат йиғиндисидан алоқанинг ишончсиз линияси бўйича узатиладиган хабарларнинг ахлитлигини текшириш воситаси сифатида фойдаланилади. Текширишнинг бу воситаси нияти бузуқ одамлар билан кўрашишга мўлжалланмаган. Чунки, бу ҳолда назорат йиғиндисининг янги қийматини қўшиб хабарни алмаштириб қўйишга уларга ҳеч ким халақит бермайди. Қабул қилувчи бунда ҳеч нарсани сезмайди.

Дайджестни ҳисоблашда, оддий назорат йиғиндисидан фарқли равишда, махфий калитлар ишлатилади. Агар дайджест олинишида фақат жўнатувчи ва қабул қилувчига маълум бўлган параметр-калитли бир томонлама хэш-функция ишлатилса, дастлабки хабарнинг ҳар қандай модификацияси дарҳол маълум бўлади.

6.5-расмда маълумотлар яхлитлигини текширишда бир томонлама хэш-функция ишлатилишининг бошқа варианти келтирилган.



6.5–расм. Маълумотлар яхлитлигини текширишда бир томонлама хэш-функциянинг ишлатиши (II-вариант).

Бу ҳолда бир томонлама хэш-функция *h(.)* параметр–калитга эга эмас, аммо у махфий калит билан тўлдирилган хабарга қўлланилади, яъни жўнатувчи дайджест m=h(M, K)ни ҳисоблайди. Қабул қилувчи дастлабки хабарни чиқариб олиб, уни ўша маълум махфий калит билан тўлдиради. Сўнгра олинган маълумотларга бир томонлама хэш-функция h(.)ни

қўллайди. Ҳисоблаш натижаси – дайджест "m" тармоқ орқали олинган дайджест "m" билан таққосланади.

Асимметрик алгоритмларга асосланган қатъий аутентификациялаш.

Қатъий аутентификациялаш протоколларида очиқ калитли асимметрик алгоритмлардан фойдаланиш мумкин. Бу ҳолда исботловчи махфий калитни билишлигини қуйидаги усулларнинг бири ёрдамида намойиш этиши мумкин:

- очиқ калитда шифрланган сўровни расшифровка қилиш;
- сўров сўзининг рақамли имзосини қўйиш.

Аутентификацияга зарур бўлган калитларнинг жуфти, хавфсизлик мулоҳазасига кўра, бошқа мақсадларга (масалан, шифрлашда) ишлатилмаслиги шарт. Очиқ калитли танланган тизим шифрланган матнни танлаш билан хужумларга, хатто бузғунчи ўзини текширувчи деб кўрсатиб ва унинг номидан ҳаракат қилганда ҳам, бардош бериши лозимлигига фойдаланувчиларни огоҳлантириш керак.

Шифрлашнинг асимметрик алгоритмларидан фойдаланиб аутентификациялаш.

Шифрлашнинг асимметрик алгоритмларидан фойдаланишга асосланган протоколга мисол тариқасида аутентификациялашнинг қуйидаги протоколини келтириш мумкин:

$$A \leftarrow B : h(r), B, P_A(r, B),$$

$$A \rightarrow B : r.$$

Қатнашувчи B тасодифий ҳолда r ни танлайди ва $x=h(r)$ қийматини ҳисоблайди (x қиймати r нинг қийматини очмасдан туриб r ни билишлигини намойиш этади), сўнгра у $e = P_A(r, B)$ қийматни ҳисоблайди. P_A орқали асимметрик шифрлаш алгоритми фараз қилинса, $h(.)$ орқали хэш-функция фараз қилинади. Қатнашувчи B ахборот хабарни қатнашувчи A га жўнатади. Қатнашувчи A $e = P_A(r, B)$ ни расшифровка қилади ва r' ва B' қийматларни олади, ҳамда $x' = h(r')$ни ҳисоблайди. Ундай кейин $x=x'$ эканлигини ва B' идентификатор ҳақиқатан қатнашувчи Bга кўрсатаётганини тасдиқловчи қатор таққослашлар бажарилади. Таққослаш муваффақиятли

ўтса қатнашувчи A "r" қатнашувчини B га узатади. Қатнашувчи B "r"ни олганидан сўнг уни биринчи хабарда жўнатган қиймати эканлигини текширади.

Кейинги мисол сифатида асимметрик шифрлашга асосланган Нидхем ва Шредернинг модификацияланган протоколини келтирамиз. Фақат аутентификациялашда ишлатилувчи Нидхем ва Шредер протоколи вариантини кўришда P_B орқали қатнашувчи Внинг очиқ калити ёрдамида шифрлаш алгоритми фараз қилинади. Протокол қуйидаги тузилмага эга:

$$A \to B : P_B(r_1, A)$$

$$A \leftarrow B : P_A(r_2, r_i)$$

$$A \leftarrow B : r_2$$

Рақамли имзодан фойдаланиш асосидаги аутентификациялаш

X.509 стандартининг тавсияларида рақамли имзо, вақт белгиси ва тасодифий сонлардан фойдаланиш асосидаги аутентификациялаш схемаси спецификацияланган. Ушбу схемани тавсифлаш учун қуйидаги белгилашларни киритамиз:

- t_A, r_A ва r_B – мос ҳолда вақт белгиси ва тасодифий сонлар;
- S_A - қатнашувчи A генерациялаган имзо;
- $cert_A$ – қатнашувчи A очиқ калитининг сертификати;
- $cert_B$ – қатнашувчи B очиқ калитининг сертификати;

Мисол тариқасида аутентификациялашнинг қуйидаги протоколларини келтирамиз:

1. Вақт белгисидан фойдаланиб бир томонлама аутентфикациялаш:

$$A \to B : cert_A, t_A, B, S_A(t_A, B)$$

Қатнашувчи B ушбу хабарни олганидан сўнг вақт белгиси t_A нинг тўғрилигини, олинган идентификатор B ни ва сертификат $cert_A$ даги очиқ калитдан фойдаланиб рақамли имзо $S_A(t_A,B)$ нинг корректлигини текширади.

2. Тасодифий сонлардан фойдаланиб бир томонлама аутентификациялаш:

$$A \leftarrow B : r_B$$

$$A \to B : cert_A, r_A, B, S_A(r_A, r_B, B)$$

Қатнашувчи B қатнашувчи A дан хабарни олиб айнан у хабарнинг адресати эканлигига ишонч ҳосил қилади; сертификат $cert_A$ дан олинган қатнашувчи A очиқ калитидан фойдаланиб очиқ кўринишда олинган r_A сони, биринчи хабарда жўнатилган r_B сони ва ўзининг идентификатори B остидаги имзо $S_A(r_A, r_B, B)$ нинг корректлигини текширади. Имзо чекилган тасодифий сон r_A очиқ матнни танлаш билан хужумни олдини олиш учун ишлатилади.

3. Тасодифий сонлардан фойдаланиб икки томонлама аутентификациялаш:

$$A \leftarrow B : r_B$$

$$A \rightarrow B : cert_A, r_A, B, S_A(r_A, r_B, B)$$

$$A \leftarrow B : cert_B, A, S_B(r_A, r_B, A)$$

Ушбу протоколдаги хабарларни ишлаш олдинги протоколдагидек бажарилади.

6.5. Фойдаланувчиларни биометрик идентификациялаш ва аутентификациялаш

Охирги вақтда инсоннинг физиологик параметрлари ва характеристикаларини, хулқининг хусусиятларини ўлчаш орқали фойдаланувчини ишончли аутентификациялашга имкон берувчи биометрик аутентификациялаш кенг тарқалмоқда.

Биометрик аутентификациялаш усуллари анъанавий усулларга нисбатан қуйидаги афзалликларга эга:

- биометрик аломатларнинг ноёблиги туфайли аутентификациялашнинг ишончлилик даражаси юқори;

- биометрик аломатларнинг соғлом шахсдан ажратиб бўлмаслиги;

- биометрик аломатларни сохталаштиришнинг қийинлиги.

Фойдаланувчини аутентификациялашда фаол ишлатиладиган биометрик алгоритмлар қуйидагилар:

- бармоқ излари;
- қўл панжасининг геометрик шакли;

- юзнинг шакли ва ўлчамлари;
- овоз хусусиятлари;
- кўз ёйи ва тўр пардасининг нақши.

Аутентификациянинг биометрик қисм тизими ишлашининг намунавий схемаси қуйидагича. Тизимда рўйхатга олинишида фойдаланувчидан ўзининг характерли аломатларини бир ёки бир неча марта намойиш қилиниши талаб этилади. Бу аломатлар (хақиқий сифатида маълум) тизим томонидан қонуний фойдаланувчининг қиёфаси сифатида рўйхатга Олинади. Фойдаланувчининг бу қиёфаси тизимда электрон шаклда сақланади ва ўзини қонуний фойдаланувчи деб даъво қилган ҳар бир одамни текширишда ишлатилади. Тақдим этилган аломатлар мажмуаси билан рўйхатга олинганларининг мослиги ёки мос келмаслигига қараб қарор қабул қилинади. Истеъмолчи нуқтаи назаридан биометрик аутенфикациялаш тизими қуйидаги иккита параметр орқали характерланади:

- хатолик инкорлар коэффициенти FRR (false-reject rate);
- хатолик тасдиқлар коэффициенти FAR (false-alarm rate).

Хатолик инкор тизим қонуний фойдаланувчи шахсини тасдиқламаганда пайдо бўлади (одатда FRR қиймати тахминан 100 дан бирни ташкил этади). *Хатолик тасдиқ* тизим ноқонуний фойдаланувчи шахсини тасдиқлаганида пайдо бўлади (одатда FAP қиймати тахминан 10000 дан бирни ташкил этади). Бу иккала коэффициент бир бири билан боғлиқ: хатолик инкор коэффициентининг ҳар бирига маълум хатолик тасдиқ коэффициенти мос келади. Мукаммал биометрик тизимда иккала хатоликнинг иккала параметри нулга тенг бўлиши шарт. Афсуски, биометрик тизим идеал эмас, шу сабабли ниманидур қурбон қилишга тўғри келади. Одатда тизимли параметрлар шундай созланадики, мос хатолик инкорлар коэффициентини аниқловчи хатолик тасдиқларнинг исталган коэффициентига эришилади.

Биометрик аутентификациялашнинг дактилосконик тизими.

Биометрик тизимларнинг аксарияти идентификациялаш параметри сифатида бармоқ изларидан фойдаланади (аутентификациянинг дактилоскопик тизими). Бундай тизимлар содда ва қулай, аутентификациялашнинг

юқори ишончлилигига эга. Бундай тизимларнинг кенг тарқалишига асосий сабаб бармоқ излари бўйича катта маълумотлар баъзасининг мавжудлигидир. Бундай тизимлардан дунёда асосан полиция, турли давлат ва баъзи банк ташкилотлари фойдаланади.

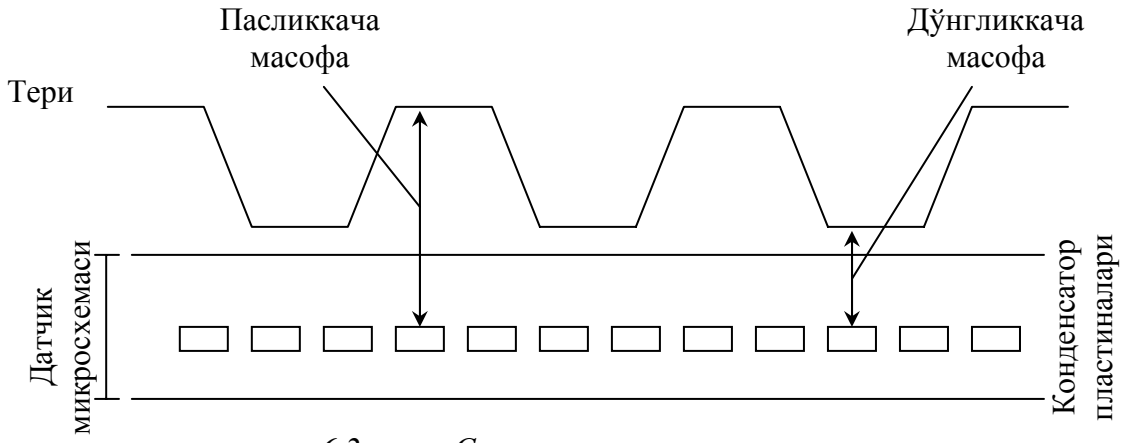
Аутентификациянинг дактилоскопик тизими қуйидагича ишлайди. Аввал фойдаланувчи рўйхатга олинади. Одатда, сканерда бармоқнинг турли холатларида сканерлашнинг бир неча варианти амалга оширилади. Табиийки, намуналар бир–биридан бироз фарқланади ва қандайдир умумлаштирилган намуна, «паспорт» шакллантирилиши талаб этилади. Натижалар аутентификациянинг маълумотлар базасида хотирланади. Аутентификациялашда сканерланган бармоқ изи маълумотлар базасидаги «паспортлар» билан таққосланади.

Бармоқ изларининг сканерлари. Бармоқ изларини сканерловчи анъанавий қурилмаларда асосий элемент сифатида бармоқнинг характерли расмини ёзувчи кичкина оптик камера ишлатилади. Аммо, дактилоскопик қурилмаларни ишлаб чиқарувчиларнинг кўпчилиги интеграл схема асосидаги сенсорли қурилмаларга эътибор бермоқдалар. Бундай тенденция бармоқ изларига асосланган аутентификациялашни қўллашнинг янги соҳаларини очади.

Бундай технологияларни ишлаб чиқувчи компаниялар бармоқ изларини олишда турли, хусусан электрик, электромагнит ва бошқа усулларни амалга оширувчи воситалардан фойдаланадилар.

Сканерлардан бири бармоқ изи тасвирини шакллантириш мақсадида тери қисмларининг сиғим қаршилигини ўлчайди. Масалан, Veridicom компаниясининг дактилоскопик қурилмаси ярим-ўтказгичли датчик ёрдамида сиғим қаршилигини аниқлаш орқали ахборотни йиғади. Сенсор ишлашининг принципи қуйидагича: ушбу асбобга қуйилган бармоқ конденсатор пластиналарининг бири вазифасини ўтайди (6.6-расм). Сенсор сиртида жойлашган иккинчи пластина конденсаторнинг 90000 сезгир пластинкали кремний микросхемасидан иборат. Сезгир сиғим датчиклари бармоқ сирти дўнгликлари ва пастликлари орасидаги электрик майдон кучининг

ўзгаришини ўлчайди. Натижада дўнгликлар ва пастликларгача бўлган масофа аниқланиб, бармоқ изи тасвири олинади.



6.2-расм. Сенсор ишлашининг принципига.

Интеграл схема асосидаги сенсорли текширишда AuthenTec компаниясида ишлатилувчи усул аниқликни яна ҳам оширишга имкон беради.

Қатор ишлаб чиқарувчилар биометрик тизимларни смарт-карталар ва карта–калитлар билан комбинациялайдилар.

Интеграл схемалар асосидаги бармоқ излари датчикларининг кичик ўлчамлари ва юқори бўлмаган нархи уларни ҳимоя тизими учун идеал интерфейсга айлантиради. Уларни калитлар учун брелокларга ўрнатиш мумкин. Натижада фойдаланувчи компьютердан бошлаб то кириш йўли, автомобиллар ва банкоматлар эшикларидан ҳимояли фойдаланишни таъминлайдиган универсал калитга эга бўлади.

Қўл панжасининг геометрик шакли бўйича аутентификациялаш тизимлари. Қўл панжаси шаклини ўқувчи қурилмалар бармоқлар узунлигини, қўл панжа қалинлиги ва юзасини ўлчаш орқали қўл панжасининг ҳажмий тасвирини яратади. Масалан, Recognition Systems компаниясининг маҳсулотлари 90 дан ортиқ ўлчамларни амалга оширади. Натижада кейинги таққослаш учун 9-хонали намуна шакллантирилади. Бу натижа қўл панжасини индивидуал сканерида ёки марказлаштирилган маълумотлар базасида сақланиши мумкин. Қўл панжасини сканерловчи қурилмалар нархининг юқорилиги ва ўлчамларининг катталиги сабабли тармоқ муҳитида камдан-кам ишлатилсада, улар қатъий хавфсизлик режимига ва шиддатли трафикка эга бўлган ҳисоблаш муҳити (сервер хоналари ҳам

бунга киради) учун қулай ҳисобланади. Уларнинг аниқлиги юқори ва инкор коэффициенти яъни инкор этилган қонуний фойдаланувчилар фоизи кичик.

Юзнинг тузилиши ва овоз бўйича аутентификацияловчи тизимлар. Бу тизимлар арзонлиги туфайли энг фойдаланувчан ҳисобланадилар, чунки аксарият замонавий компьютерлар видео ва аудео воситаларига эга. Бу синф тизимлари телекоммуникация тармоқларида масофадаги фойдаланувчи субъектни идентификациялаш учун ишлатилади. *Юз тузилишини сканерлаш технологияси* бошқа биометрик технологиялар яроқсиз бўлган иловалар учун тўғри келади. Бу ҳолда шахсни идентификациялаш ва верификациялаш учун кўз, бурун ва лаб хусусиятлари ишлатилади. Юз тузилишини аниқловчи қурилмаларни ишлаб чиқарувчилар фойдаланувчини идентификациялашда ҳусусий математик алгоритмлардан фойдаланадилар.

Маълум бўлишича, кўпгина ташкилотларнинг ҳодимлари юз тузилишини сканерловчи қурилмаларга ишонмайдилар. Уларнинг фикрича камера уларни расмга олади, сўнгра суратни монитор экранига чиқаради. Камеранинг сифати эса паст бўлиши мумкин. Ундан ташқари юз тузилишини сканерлаш – биометрик аутентификациялаш усуллари ичида ягона, текширишга рухсатни талаб қилмайдиган (яширинган камера ёрдамида амалга оширилиши мумкин) усул ҳисобланали.

Таъкидлаш лозимки, юз тузилишини аниқлаш технологияси янада такомиллаштирилишни талаб этади. Юз тузилишини аниқловчи аксарият алгоритмлар қуёш ёруғлиги жадаллигининг кун бўйича тебраниши натижасидаги ёруғлик ўзгаришига таъсирчан бўладилар. Юз ҳолатининг ўзгариши ҳам аниқлаш натижасига таъсир этади. Юз ҳолатининг 45^0 га ўзгариши аниқлашни самарасиз бўлишига олиб келади.

Овоз бўйича аутентификациялаш тизимлари. Бу тизимлар арзонлиги туфайли фойдаланувчан ҳисобланадилар. Ҳусусан уларни кўпгина шахсий компьютерлар стандарт комплектидаги ускуна (масалан микрофонлар) билан бирга ўрнатиш мумкин. Овоз бўйича аутентификациялаш тизимлари ҳар бир одамга ноёб бўлган баландлиги, модуляцияси ва товуш частотаси каби овоз хусусиятларига асосланади.

Овозни аниқлаш нутқни аниқлашдан фарқланади. Чунки нутқни аниқловчи технология абонент сўзини изохласа, овозни аниқлаш технологияси сўзловчининг шахсини тасдиқлайди. Сўзловчи шахсини тасдиқлаш баъзи чегараланишларга эга. Турли одамлар ўхшаш овозлар билан гапириши мумкин, ҳар қандай одамнинг овози вақт мобайнида кайфияти, ҳиссиётлик ҳолати ва ёшига боғлиқ ҳолда ўзгариши мумкин. Унинг устига телефон аппаратларнинг турли-туманлиги ва телефон орқали боғланишларининг сифати сўзловчи шахсини аниқлашни қийинлаштиради. Шу сабабли овоз бўйича аниқлашни юз тузилишини ёки бармоқ изларини аниқлаш каби бошқа биометриклар билан биргаликда амалга ошириш мақсадга мувофиқ ҳисобланади.

Кўз ёйи тўр пардасининг шакли бўйича аутентификациялаш тизими. Бу тизимларни иккита синфга ажратиш мумкин:

- кўз ёйи расмидан фойдаланиш;
- кўз тўр пардаси қон томирлари расмидан фойдаланиш.

Одам кўз пардаси аутентификация учун ноёб объект ҳисобланади. Кўз туби қон томирларининг расми ҳатто эгизакларда ҳам фарқланади. Идентификациялашнинг бу воситаларидан хавфсизликнинг юқори даражаси талаб этилганида (масалан ҳарбий ва мудофаа объектларининг режимли зоналарида) фойдаланилади.

Биометрик ёндашиш “ким бу ким” эканлигини аниқлаш жараёнини соддалаштиришга имкон беради. Дактилоскопик сканерлар ва овозни аниқловчи қурилмалардан фойдаланиш ходимларни тармоққа киришларида мураккаб паролларни эслаб қолишдан халос этади. Қатор компаниялар корхона масштабидаги бир мартали аутентификация SSO (Single Sign-On) га биометрик имкониятларни интеграциялайдилар. Бундай бириктириш тармоқ маъмурларига паролларни бир мартали аутентификациялаш хизматини биометрик технологиялар билан алмаштиришга имкон беради. Шахсни биометрик аутентификациялашнинг биринчилар қаторида кенг тарқалган соҳаларидан бири мобил тизимлари бўлди. Муаммо фақат компьютер ўғирланишидаги йўқотишларда эмас, балки ахборот тизимининг бузилиши катта зарарга олиб келиши мумкин. Ундан ташқари, ноутбуклар

дастурий боғланиш (мобил компьютерларда сақланувчи пароллар ёрдамида) орқали корпоратив тармоқдан фойдаланишни тез-тез амалга оширади. Бу муаммоларни кичик, арзон ва катта энергия талаб этмайдиган бармоқ излари датчиклари ечишга имкон беради. Бу қурилмалар мос дастурий таъминот ёрдамида ахборотдан фойдаланишнинг мобил компьютерда сақланаётган тўртта сатхи - рўйхатга олиш, экранни сақлаш режимидан чиқиш, юклаш ва файлларни дешифрациялаш учун аутентификацияни бажаришга имкон беради.

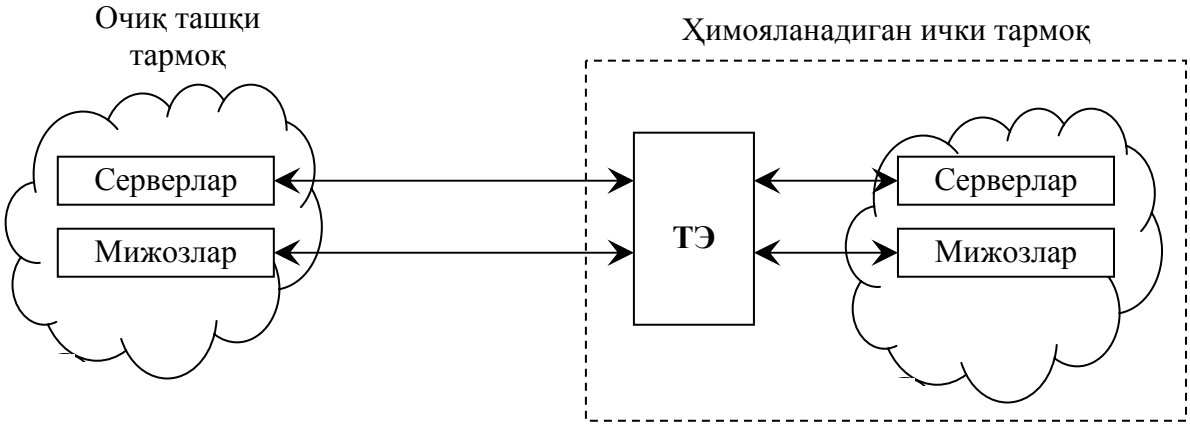
Фойдаланувчини биометрик аутентификациялаш махфий калитдан фойдаланишни модул кўринишида шифрлашда жиддий аҳамиятга эга бўлиши мумкин. Бу модул ахборотдан фақат хақиқий хусусий калит эгасининг фойдаланишига имкон беради. Сўнгра калит эгаси ўзининг махфий калитини ишлатиб хусусий тармоқлар ёки Internet орқали узатилаётган ахборотни шифрлаши мумкин.

VII боб. ТАРМОҚЛАРАРО ЭКРАН ТЕХНОЛОГИЯСИ

7.1. Тармоқлараро экранларнинг ишлаш хусусиятлари

Тармоқлараро экран (ТЭ) - *брандмауэр* ёки *firewall системаси* деб ҳам аталувчи тармоқлараро ҳимоянинг ихтисослаштирилган комплекси. Тармоқлараро экран умумий тармоқни икки ёки ундан кўп қисмларга ажратиш ва маълумот пакетларини чегара орқали умумий тармоқнинг бир қисмидан иккинчисига ўтиш шартларини белгиловчи қоидалар тўпламини амалга ошириш имконини беради. Одатда, бу чегара корхонанинг корпоратив (локал) тармоғи ва Internet глобал тармоқ орасида ўтказилади. Тармоқлараро экранлар гарчи корхона локал тармоғи уланган корпоратив интратармоғидан қилинувчи ҳужумлардан ҳимоялашда ишлатилишлари мумкин бўлсада, одатда улар корхона ички тармоғини Internet глобал тармоқдан суқилиб киришдан ҳимоялайди. Аксарият тижорат ташкилотлари учун тармоқлараро экранларнинг ўрнатилиши ички тармоқ хавфсизлигини таъминлашнинг зарурий шарти ҳисобланади.

Рухсат этилмаган тармоқлараро фойдаланишга қарши таъсир кўрсатиш учун тармоқлараро экран ички тармоқ ҳисобланувчи ташкилотнинг ҳимояланувчи тармоғи ва ташқи ғаним тармоқ орасида жойланиши лозим (7.1-расм). Бунда бу тармоқлар орасидаги барча алоқа фақат тармоқлараро экран орқали амалга оширилиши лозим. Ташкилий нуқтаи



7.1-расм. Тармоқлараро экранни улаш схемаси.

назаридан тармоқлараро экран ҳимояланувчи тармоқ таркибига киради.

Ички тармоқнинг кўпгина узелларини бирданига ҳимояловчи тармоқлараро экран қуйидаги иккита вазифани бажариши керак:

- ташқи (ҳимояланувчи тармоққа нисбатан) фойдаланувчиларнинг корпоратив тармоқнинг ички ресурсларидан фойдаланишини чегаралаш. Бундай фойдаланувчилар қаторига тармоқлараро экран ҳимояловчи маълумотлар базасининг серверидан фойдаланишга уринувчи шериклар, масофадаги фойдаланувчилар, хакерлар, ҳатто компаниянинг ходимлари киритилиши мумкин;

- ҳимояланувчи тармоқдан фойдаланувчиларнинг ташқи ресурслардан фойдаланишларини чегаралаш. Бу масаланинг ечилиши, масалан, сервердан хизмат вазифалари талаб этмайдиган фойдаланишни тартибга солишга имкон беради.

Ҳозирда ишлаб чиқарилаётган тармоқлараро экранларнинг тавсифларига асосланган ҳолда, уларни қуйидаги асосий аломатлари бўйича туркумлаш мумкин:

OSI модели сатҳларида ишлаши бўйича:

- пакетли фильтр (экранловчи маршрутизатор – screening router);
- сеанс сатҳи шлюзи (экранловчи транспорт);
- татбиқий шлюз (application gateway);
- эксперт сатҳи шлюзи (stateful inspection firewall).

Ишлатиладиган технология бўйича:

- протокол ҳолатини назоратлаш (Stateful inspection);
- воситачилар модуллари асосида (proxy);

Бажарилиши бўйича:

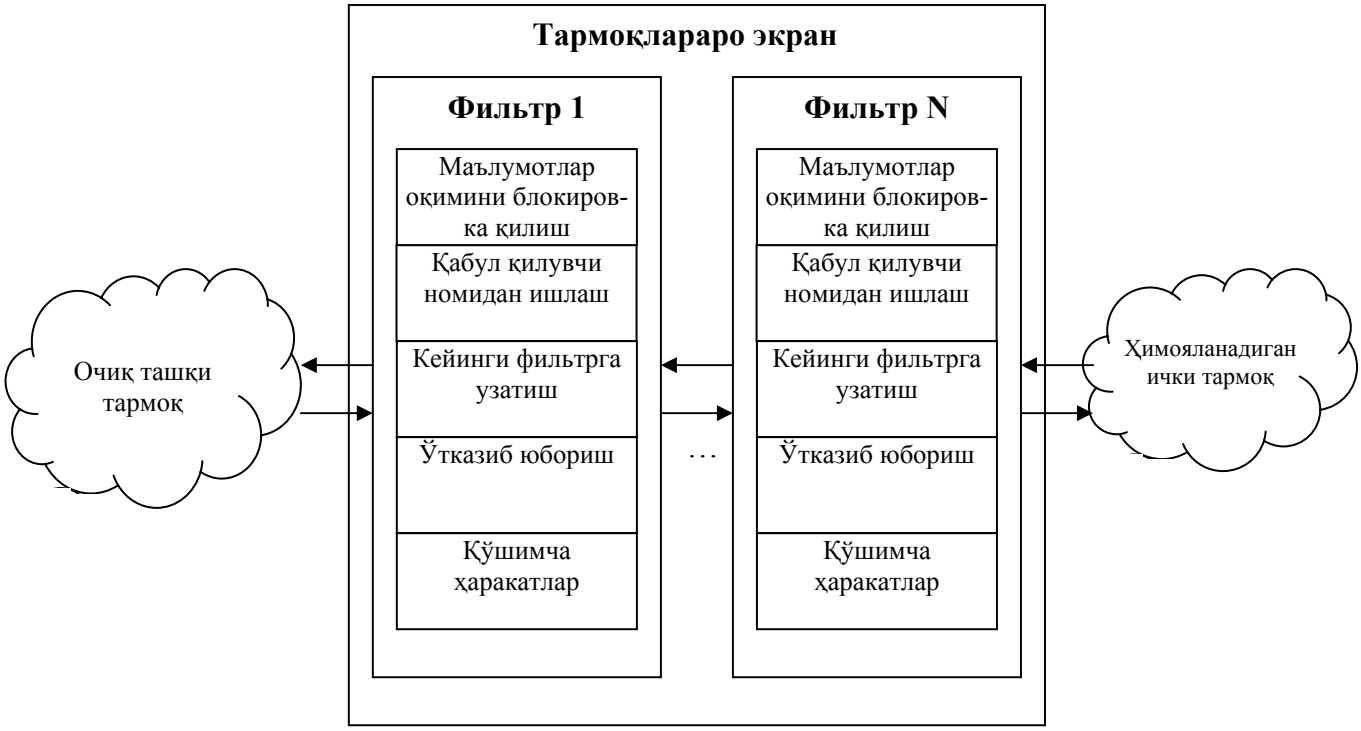
- аппарат-дастурий;
- дастурий;

Уланиш схемаси бўйича;

- тармоқни умумий ҳимоялаш схемаси;
- тармоқ сегментлари ҳимояланувчи берк ва тармоқ сегментлари ҳимояланмайдиган очиқ схема;

- тармоқнинг берк ва очиқ сегментларини алоҳида ҳимояловчи схема.

Трафикларни фильтрлаш. Ахборот оқимларини фильтрлаш уларни экран орқали, баъзида қандайдир ўзгартиришлар билан, ўтказишдан иборат. Фильтрлаш қабул қилинган хавфсизлик сиёсатига мос келувчи, экранга олдиндан юкланган қоидалар асосида амалга оширилади. Шу сабабли тармоқлараро экранни ахборот оқимларини ишловчи фильтрлар кетма-кетлиги сифатида тасаввур этиш қулай (7.2-расм).



7.2-расм. Тармоқлараро экран тузилмаси.

Фильтрларнинг ҳар бири қуйидаги ҳаракатларни бажариш орқали фильтрлашнинг алоҳида қоидаларини изоҳлашга аталган:

1. Ахборотни изоҳланувчи қоидалардаги берилган мезонлар бўйича таҳлиллаш, масалан, қабул қилувчи ва жўнатувчи адреслари ёки ушбу ахборот аталган илова хили бўйича.

2. Изоҳланувчи қоидалар асосида қуйидаги ечимлардан бирини қабул қилиш:

- маълумотларни ўтказмаслик;

- маълумотларни қабул қилувчи номидан ишлаш ва натижани жўнатувчига қайтариш;

- тахлиллашни давом эттириш учун маълумотларни кейинги фильтрга узатиш;

- кейинги фильтрларга эътибор қилмай маълумотларни узатиш.

Фильтрлаш қоидалари воситачилик функцияларига оид қўшимча, масалан маълумотларни ўзгартириш, ходисаларни қайдлаш ва ҳ. каби ҳаракатларни ҳам бериши мумкин. Мос ҳолда, фильтрлаш қоидалари қуйидагиларнинг амалга оширилишини таъминловчи шартлар рўйхатини аниқлайди:

- маълумотларни кейинги узатишга рухсат бериш ёки рухсат бермаслик;

- ҳимоялашнинг қўшимча функцияларини бажариш.

Ахборот оқимини тахлиллаш мезони сифатида қуйидаги параметрлардан фойдаланиш мумкин:

- таркибида тармоқ адреслари, идентификаторлар, интерфейслар адреси, портлар номери ва бошқа муҳим маълумотлар бўлган хабар пакетларининг хизматчи хошиялари;

- масалан, компьютер вируслари борлигига текширилувчи хабар пакетларининг бевосита таркиби;

- ахборот оқимининг ташқи характеристикалари, масалан, вақт ва частота характеристикалари маълумотлар ҳажми ва ҳ.

Ишлатилувчи тахлиллаш мезонлари фильтрлашни амалга оширувчи OSI моделининг сатҳларига боғлиқ. Умумий ҳолда, пакетни фильтрлашни амалга оширувчи OSI моделининг сатҳи қанчалик юқори бўлса, таъминланувчи ҳимоялаш даражаси ҳам шунчалик юқори бўлади.

Воситачилик функцияларининг бажарилиши. Тармоқлараро экран воситачилик функцияларини *экранловчи агентлар* ёки *воситачи дастурлар* деб аталувчи махсус дастурлар ёрдамида бажаради. Бу дастурлар резидент дастурлар ҳисобланади ва ташқи ва ички тармоқ орасида хабарлар пакетини бевосита узатишни тақиқлайди.

Ташқи тармоқдан ички тармоқнинг ва аксинча фойдаланиш зарурияти туғилганда аввал тармоқлараро экран компьютерида ишловчи воситачи-дастур билан мантиқий уланиш ўрнатилиши лозим. Воситачи-дастур

сўралган тармоқлараро алоқанинг жоизлигини текширади ва ижобий натижада ўзи суралган компьютер билан алоҳида уланиш ўрнатади. Сўнгра ташқи ва ички тармоқ компьютерлари орасида ахборот алмашиш, хабарлар оқимини фильтрлашни ҳамда бошқа ҳимоялаш функцияларини бажарувчи дастурий воситачи орқали амалга оширилади.

Таъкидлаш лозимки, тармоқлараро экран фильтрлаш функциясини воситачи-дастур иштирокисиз амалга ошириб, ташқи ва ички тармоқ орасида ўзаро алоқанинг шаффофлигини таъминлаши мумкин. Шу билан бирга воситачи дастурлар хабарлар оқимини фильтрлашни амалга оширмаслиги ҳам мумкин.

Умуман, воситачи-дастурлар, хабарлар оқимини шаффоф узатилишини блокировка қилган ҳолда, қуйидаги функцияларни бажариши мумкин:

- узатилувчи ва қабул қилинувчи маълумотларнинг ҳақиқийлигини текшириш;
- ички тармоқ ресурсларидан фойдаланишни чегаралаш;
- ташқи тармоқ ресурсларидан фойдаланишни чегаралаш;
- ташқи тармоқдан сўралувчи маълумотларни кэшлаш;
- хабарлар оқимини фильтрлаш ва ўзгартириш, масалан, вирусларни динамик тарзда қидириш ва ахборотни шаффоф шифрлаш;
- фойдаланувчиларни идентификациялаш ва аутентификациялаш;
- ички тармоқ адресларини трансляциялаш;
- ходисаларни қайдлаш, ходисаларга реакция кўрсатиш, хамда қайдланган ахборотни тахлиллаш ва ҳисоботларни генерациялаш.

Узатилувчи ва қабул қилинувчи маълумотларнинг ҳақиқийлигини текшириш нафақат электрон хабарларни, балки сохталаштирилиши мумкин бўлган мигрицияланувчи дастурларни (Java, Active X Controls) аутентифкациялаш учун долзарб ҳисобланади. Хабар ва дастурларнинг ҳақиқийлигини текшириш уларнинг рақамли имзосини текширишдан иборатдир.

Ички тармоқ ресурсларидан фойдаланишни чегаралаш усуллари операцион тизим сатҳида мададланувчи чегаралаш усулларидан фарқ қилмайди.

*Ташқи тармоқ ресурсларидан фойдаланишни чегарлаш*да кўпинча қуйидаги ёндашишлардан бири ишлатилади:

- фақат ташқи тармоқдаги берилган адрес бўйича фойдаланишга рухсат бериш;

- янгиланувчи ножоиз адреслар руйхати бўйича суровларни фильтрлаш ва ўринсиз калит сўзлари бўйича ахборот ресурсларини қидиришни блокировка қилиш:

- маъмур томонидан ташқи тармоқнинг қонуний ресурсларини брандмауэрнинг дискли хотирасида тўплаш ва янгилаш ва ташқи тармоқдан фойдаланишни тўла тақиқлаш.

Ташқи тармоқдан сўралувчи *маълумотларни кэшлаш* махсус воситачилар ёрдамида мададланади. Ички тармоқ фойдаланувчилари ташқи тармоқ ресурсларидан фойдаланганларида барча ахборот, proxy-сервер деб аталувчи брандмауэр қаттиқ диски маконида тўпланади. Шу сабабли, агар навбатдаги сўровда керакли ахборот proxy-серверда бўлса, воситачи уни ташқи тармоққа мурожаатсиз тақдим этади. Бу фойдаланишни жиддий тезлаштиради. Маъмурга фақат proxy-сервер таркибини вақти-вақти билан янгилаб туриш вазифаси қолади.

Кэшлаш функцияси ташқи тармоқ ресурсларидан фойдаланишни чегаралашда муваффақиятли ишлатилиши мумкин. Бу ҳолда ташқи тармоқнинг барча қонуний ресурслари маъмур томонидан proxy-серверда тўпланади ва янгиланади. Ички тармоқ фойдаланувчиларига фақат proxy-сервернинг ахборот ресурсларидан фойдаланишга рухсат берилади, ташқи тармоқ ресурсларидан бевосита фойдаланиш эса манн қилинади.

Хабарлар оқимини фильтрлаш ва ўзгартириш воситачи томонидан қоидаларнинг берилган тўплами ёрдамида бажарилади. Бунда воситачи-дастурларнинг икки хили фарқланади:

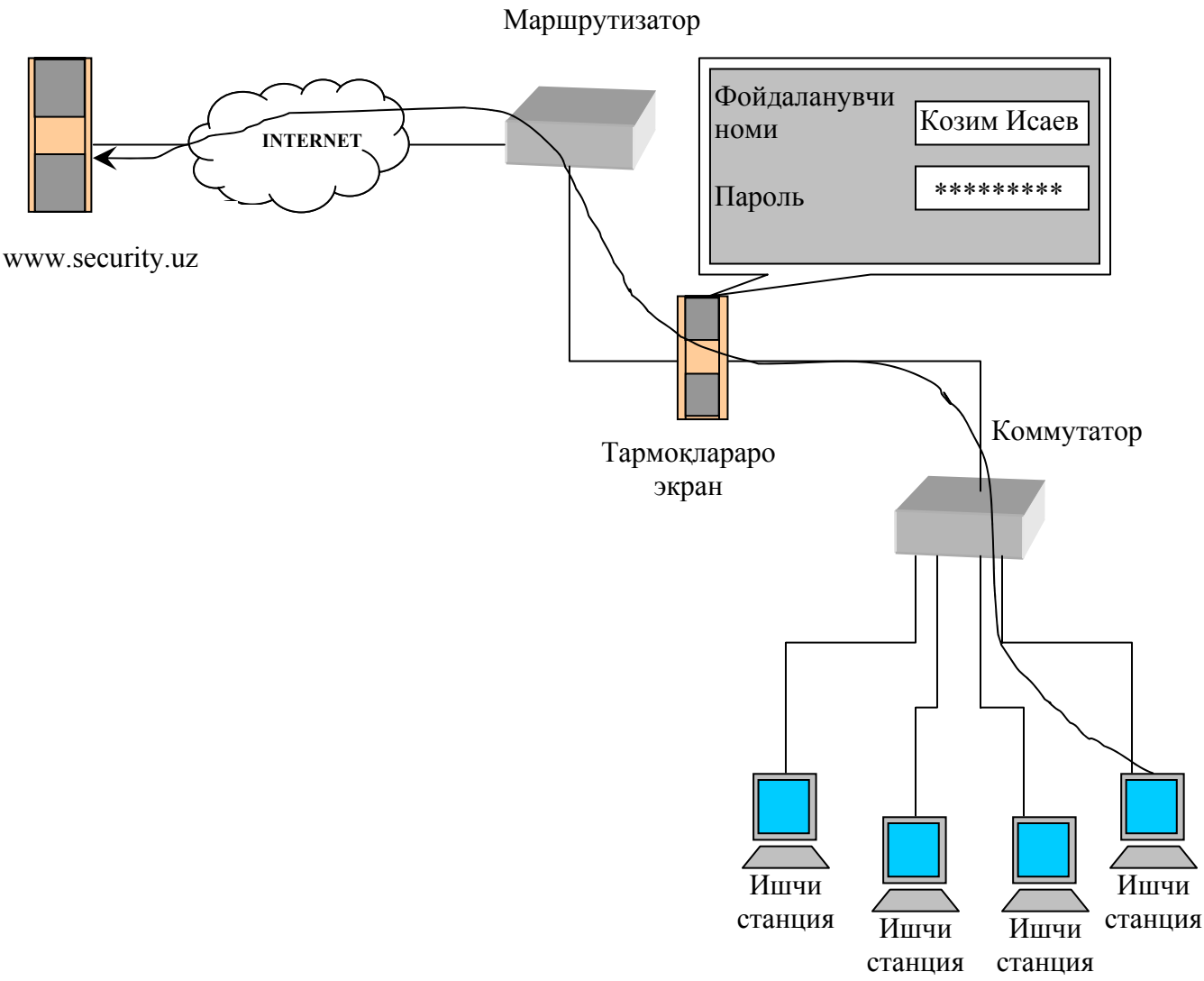
- сервис турини аниқлаш учун хабарлар оқимини тахлиллашга мўлжалланган экранловчи агентлар, масалан, FTP, HTTP, Telnet;

- барча хабарлар оқимини ишловчи универсал экранловчи агентлар, масалан, компьютер вирусларини қидириб зарарсизлантиришга ёки маълумотларни шаффоф шифрлашга мўлжалланган агентлар.

Дастурий воситачи унга келувчи маълумотлар пакетини тахлиллайди ва агар қандайдир объект берилган мезонларга мос келмаса, воситачи унинг

кейинги силжишини блокировка қилади ёки мос ўзгаришини, масалан, ошкор қилинган компьютер вирусларни зарарсизлантиришни бажаради. Пакетлар таркибини тахлиллашда экранловчи агентнинг ўтувчи файлли архивларни автоматик тарзда оча олиши муҳим ҳисобланади.

Фойдаланувчиларни идентификациялаш ва аутентификациялаш баъзида оддий идентификаторни (исм) ва паролни тақдим этиш билан амалга оширилади (7.3-расм). Аммо бу схема хавфсизлик нуқтаи назаридан заиф ҳисобланади, чунки паролни бегона шахс ушлаб қолиб ишлатиши мумкин. Internet тармоғидаги кўпгина можаролар қисман анъанавий кўп марта ишлатилувчи паролларнинг заифлигидан келиб чиққан.



9.3–расм. Пароль бўйича фойдаланувчини аутентификациялаш схемаси

Аутентификациялашнинг ишончлироқ усули – бир марта ишлатилувчи пароллардан фойдаланишдир. Бир мартали паролларни генерациялашда

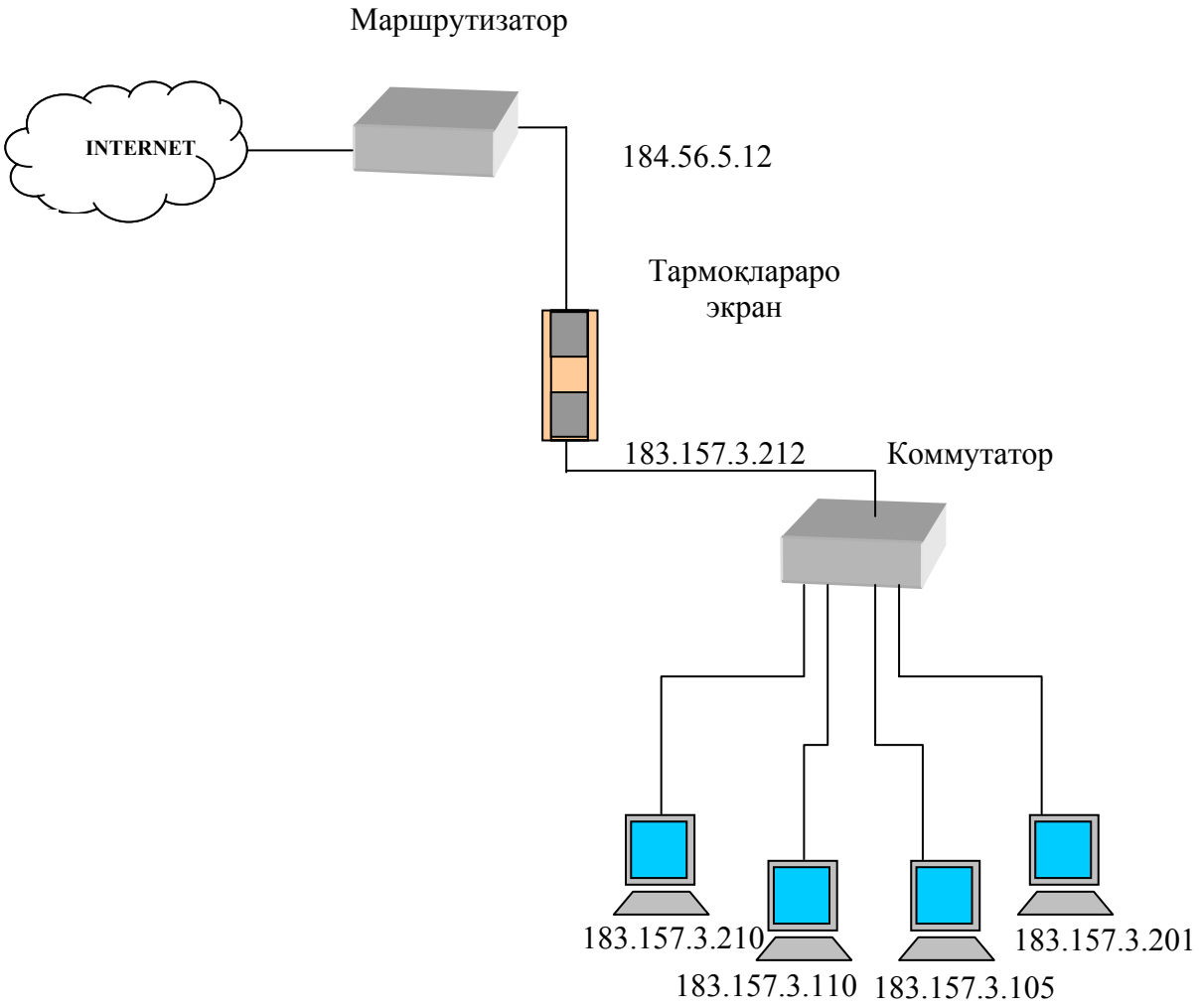
аппарат ва дастурий воситалардан фойдаланилади. Аппарат воситалари компьютернинг слотига ўрнатилувчи қурилма бўлиб, уни ишга тушириш учун фойдаланувчи қандайдир махфий ахборотни билиши зарур. Масалан, смарт-карта ёки фойдаланувчи токени ахборотни генерациялайди ва бу ахборотни хост анъанавий парол ўрнида ишлатади. Смарт-карта ёки токен хостнинг аппарат ва дастурий таъминоти билан бирга ишлаши сабабли, генерацияланувчи парол ҳар бир сеанс учун ноёб бўлади.

Ишончли орган, масалан калитларни тақсимлаш маркази томонидан берилувчи рақамли сертификатларни ишлатиш ҳам қулай ва ишончли. Кўпгина воситачи дастурлар шундай ишлаб чиқиладики, фойдаланувчи фақат тармоқлараро экран билан ишлаш сеансининг бошида аутентификациялансин. Бундан кейин маъмур белгиланган вақт мобайнида ундан қўшимча аутентификацияланиш талаб этилмайди.

Тармоқлараро экранлар тармоқдан фойдаланишни бошқаришни марказлаштиришлари мумкин. Демак, улар кучайтирилган аутентификациялаш дастурлари ва қурилмаларини ўрнатишга муносиб жой ҳисобланади. Гарчи кучайтирилган аутентификация воситалари ҳар бир хостда ишлатилиши мумкин бўлсада, уларнинг тармоқлараро экранларда жойлаштириш қулай. Кучайтирилган аутентификациялаш чораларидан фойдаланувчи тармоқлараро экранлар бўлмаса, Telnet ёки FTP каби иловаларнинг аутентификацияланмаган трафиги тармоқнинг ички тизимларига тўғридан-тўғри ўтиши мумкин.

Қатор тармоқлараро экранлар аутентификациялашнинг кенг тарқалган усулларидан бири – Kerberosни мададлайди. Одатда, аксарият тижорат тармоқлараро экранлар аутентификациялашнинг турли схемаларини мададлайди. Бу эса тармоқ хавфсизлиги маъмурига ўзининг шароитига қараб энг мақбул схемани танлаш имконини беради.

Ички тармоқ адресларини трансляциялаш. Кўпгина хужумларни амалга оширишда нияти бузуқ одамга қурбонининг адресини билиш керак бўлади. Бу адресларни ҳамда бутун тармоқ топологиясини беркитиш учун тармоқлараро экранлар энг муҳим вазифани – ички тармоқ адресларини трансляциялашни бажаради (7.4-расм).



7.4–расм. Тармоқ адресларини трансляциялаш

Бу функция ички тармоқдан ташқи тармоққа узатилувчи барча пакетларга нисбатан бажарилади. Бундай пакетлар учун жўнатувчи компьютерларнинг IP-адреслари битта "ишончли" IP адресга автоматик тарзда ўзгартирилади.

Ички тармоқ адресларини трансляциялаш иккита усул-динамик ва статик усулларда амалга оширилиши мумкин. Динамик усулда адрес узелга тармоқлараро экранга мурожаат онида ажратилади. Уланиш тугалланганидан сўнг адрес бўшайди ва уни корпоратив тармоқнинг бошқа узели ишлатиши мумкин. Статик усулда узел адреси барча чиқувчи пакетлар узатиладиган тармоқлараро экраннинг битта адресига доимо боғланади. Тармоқлараро экраннинг IP-адреси ташқи тармоққа тушувчи ягона фаол IP-адресга айланади. Натижада, ички тармоқдан чиқувчи барча пакетлар тармоқлараро экрандан жўнатилган бўлади. Бу авторизацияланган ички

тармоқ ва хавфли бўлиши мумкин бўлган ташқи тармоқ орасида тўғридан-тўғри алоқани истисно қилади.

Бундай ёндашишда ички тармоқ топологияси ташқи фойдаланувчилардан яширинган, демак, рухсатсиз фойдаланиш масаласи қийинлашади. Адресларни трансляциялаш тармоқ ичида ташқи тармоқ, масалан Internetдаги адреслаш билан келишилмаган адреслашнинг хусусий тизимига эга бўлишига имкон беради. Бу ички тармоқнинг адрес маконини кенгайтириш ва ташқи адрес танқислиги муаммосини самарали ечади.

Ходисаларни қайдлаш, ходисаларга реакция кўрсатиш, ҳамда қайдланган ахборотни тахлиллаш ва ҳисоботларни генерациялаш тармоқлараро экранларнинг муҳим вазифалари ҳисобланади. Корпоратив тармоқни ҳимоялаш тизимининг жиддий элементи сифатида тармоқлараро экран барча ҳаракатларни рўйхатга олиш имкониятига эга. Бундай ҳаракатларга нафақат тармоқ пакетларини ўтказиб юбориш ёки блокировка қилиш, балки хавфсизлик маъмури томонидан фойдаланишни қоидасини ўзгартириш ва ҳ. ҳам тааллуқли. Бундай руйхатга олиш зарурият туғилганда (хавфсизлик можароси пайдо бўлганида ёки суд инстанцияларига ёки ички тергов учун далилларни йиғишда) яратилувчи журналларга мурожаат этишга имкон беради.

Шубҳали ходисалар (alarm) хусусидаги сигналларни қайдлаш тизими тўғри созланганида тармоқлараро экран ёки тармоқ хужумга дучор бўлганлиги ёки зондланганлиги тўғрисидаги батафсил ахборотни бериши мумкин. Тармоқдан фойдаланиш ва унинг зондланганлигининг исботи статистикасини йиғиш қатор сабабларга кўра муҳимдир. Аввало. тармоқлараро экраннинг зондланишга ва хужумларга бардошлигини аниқ билиш зарур ва тармоқлараро экранни ҳимоялаш тадбирларининг адэкватлигини аниқлаш лозим. Ундан ташқари, тармоқдан фойдаланиш статистикаси тармоқ асбобускуналарига ва дастурларига талабларни ифодалаш мақсадида хавф-хатарни тадқиқлаш ва тахлиллашда дастлабки маълумотлар сифатида муҳим ҳисобланади.

Кўпгина тармоқлараро экранлар статистикани қайдловчи, йиғувчи ва тахлилловчи қувватли тизимга эга. Мижоз ва сервер адреси, фойдаланувчилар идентификатори, сеанс вақтлари, уланиш вақтлари, узатилган ва қабул

қилинган маълумотлар сони, маъмур ва фойдаланувчилар ҳаракатлари бўйича ҳисоб олиб борилиши мумкин. Ҳисоб тизимлари статистикани тахлиллашга имкон беради ва маъмурларга батафсил ҳисоботларни тақдим этади. Тармоқлараро экранлар махсус протоколлардан фойдаланиб, маълум ходисалар тўғрисида реал вақт режимида масофадан хабар беришни бажариши мумкин.

Рухсатсиз ҳаракатларни қилишга уринишларни аниқланишига бўладиган мажбурий реакция сифатида маъмурнинг хабари, яъни огоҳлантирувчи сигналларни бериш белгиланиши лозим. Хужум қилинганлиги аниқланганда огоҳлантирувчи сигналларни юборишга қодир бўлмаган тармоқлараро экранни тармокларо ҳимоянинг самарали воситаси деб бўлмайди.

7.2. Тармоқлараро экранларнинг асосий компонентлари

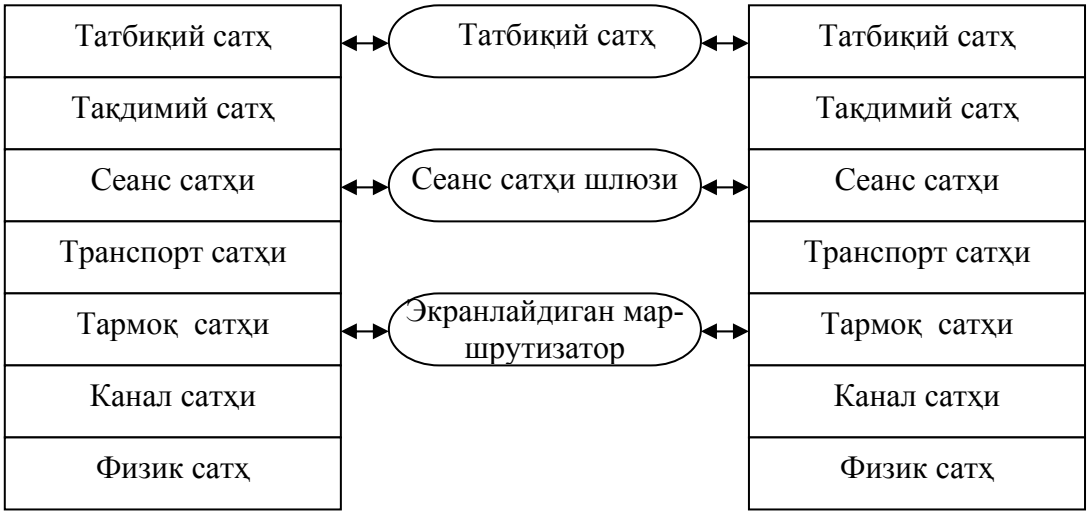
Тармоқлараро экранлар тармоқлараро алоқа хавфсизлигини OSI моделининг турли сатҳларида мададлайди. Бунда эталон моделнинг турли сатҳларида бажариладиган ҳимоя функциялари бир-биридан жиддий фарқланади. Шу сабабли, тармоқлараро экранлар комплексини, ҳар бири OSI моделининг алоҳида сатҳига мўлжалланган, бўлинмайдиган экранлар мажмуи кўринишида тасаввур этиш мумкин.

Экранлар комплекси кўпинча эталон моделнинг тармоқ, сеанс, татбиқий сатҳларида ишлайди. Мос ҳолда, қуйидаги бўлинмайдиган брандмауэрлар фарқланади (7.5-расм).

- экранловчи маршрутизатор;
- сеанс сатҳи шлюзи (экранловчи транспорт);
- татбиқий сатҳ шлюзи (экранловчи шлюз).

Тармоқларда ишлатиладиган протоколлар (TCP/IP, SPX/IPX) OSI эталон моделига батамом мос келмайди, шу сабабли санаб ўтилган экранлар хили функцияларини амалга оширишда эталон моделининг қўшни сатҳларини ҳам қамраб олишлари мумкин. Масалан, татбиқий экран хабарларнинг ташқи тармоққа узатилишида уларни автоматик тарзда шифрлаш-

ни, ҳамда қабул қилинувчи криптографик беркитилган маълумотларни автоматик тарзда расшифровка қилишни амалга ошириши мумкин. Бу ҳолда бундай экран OSI моделининг нафақат татбиқий сатҳида, балки тақдимий сатҳида ҳам ишлайди.



7.5-расм. OSI моделининг алоҳида сатҳларида ишлайдиган тармоқлараро экранлар тури

Сеанс сатҳи шлюзи ишлашида OSI моделининг транспорт ва тармоқ сатҳларини қамраб олади. Экранловчи маршрутизатор хабарлар пакетини тахлиллашда уларнинг нафақат тармоқ, балки транспорт сатҳи сарлавҳаларини ҳам текширади.

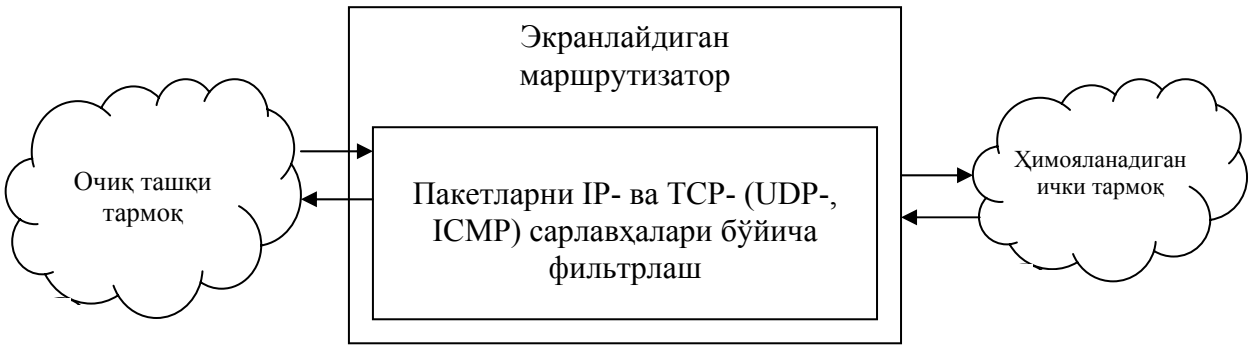
Юқорида келтирилган тармоқлараро экранларнинг хиллари ўзининг афзалликлари ва камчиликларига эга. Ишлатиладиган брандмауэрларнинг кўпчилиги ёки татбиқий шлюзлар, ёки экранловчи маршрутизаторлар бўлиб, тармоқлараро алоқанинг тўлиқ хавфсизлигини таъминламайди. Ишончли ҳимояни эса фақат ҳар бири экранловчи маршрутизатор, сеанс сатҳи шлюзи, ҳамда татбиқий шлюзни бирлаштирувчи тармоқлараро экранларнинг комплекси таъминлайди.

Экранловчи маршрутизатор (screening router) (пакетли фильтр (packet filter) деб ҳам аталади) хабарлар пакетини фильтрлашга аталган ва ички ва ташқи тармоқлар орасида шаффоф алоқани таъминлайди. У OSI моделининг тармоқ сатҳида ишлайди, аммо ўзининг айрим функцияларини бажаришида эталон моделининг транспорт сатҳини ҳам қамраб олиши мумкин.

Маълумотларни ўтказиш ёки бракка чиқариш хусусидаги қарор фильтрлашнинг берилган қоидаларига биноан ҳар бир пакет учун мустақил қабул қилинади. Қарор қабул қилишда тармоқ ва транспорт сатҳлари пакетларининг сарлавҳалари тахлил этилади (7.6-расм).

Ҳар бир пакетнинг IP- ва TCP/UDP – сарлавҳаларининг тахлилланувчи ҳошиялари сифатида қуйидагилар ишлатилиши мумкин:

- жўнатувчи адреси;
- қабул қилувчи адреси;
- пакет ҳили;
- пакетни фрагментлаш байроғи;
- манба порти номери;
- қабул қилувчи порт номери.



7.6-расм. Пакетли фильтрни ишлаш схемаси

Биринчи тўртта параметр пакетнинг IP-сарлавҳасига, кейингилари эса TCP-ёки UDP сарлавҳасига тааллуқли. Жўнатувчи ва қабул қилувчи адреслари IP-адреслар ҳисобланади. Бу адреслар пакетларни шакллантиришда тўлдирилади ва уни тармоқ бўйича узатганда ўзгармайди.

Пакет хили ҳошиясида тармоқ сатҳига мос келувчи ICMP протокол коди ёки тахлилланувчи IP-пакет тааллуқли бўлган транспорт сатҳи протоколининг (TCP ёки UDP) коди бўлади.

Пакетни фрагментлаш байроғи IP-пакетлар фрагментлашининг борлиги ёки йўқлигини аниқлайди. Агар таҳлилланувчи пакет учун фрагментлаш байроғи ўрнатилган бўлса, мазкур пакет фрагментланган IP-пакетнинг қисм пакети ҳисобланади.

Манба ва қабул қилувчи портлари номерлари TCP ёки UDP драйвер томонидан ҳар бир жўнатилувчи хабар пакетларига қўшилади ва жўнатувчи иловасини, ҳамда ушбу пакет аталган иловани бир маънода идентификациялайди. Портлар номерлари бўйича фильтрлаш имконияти учун юқори сатҳ протоколларига порт номерларини ажратиш бўйича тармоқда қабул қилинган келишувни билиш лозим.

Ҳар бир пакет ишланишида экранловчи маршрутизатор берилган қоидалар жадвалини, пакетнинг тўлиқ ассоциациясига мос келувчи қоидани топгунича, кетма-кет кўриб чиқади. Бу ерда ассоциация деганда берилган пакет сарлавҳаларида кўрсатилган параметрлар мажмуи тушунилади. Агар экранловчи маршрутизатор жадвалдаги қоидаларнинг бирортасига ҳам мос келмайдиган пакетни олса, у, хавфсизлик нуқтаи назаридан, уни брака чиқаради.

Пакетли фильтрлар аппарат ва дастурий амалга оширилиши мумкин. Пакетли фильтр сифатида оддий маршрутизатор, ҳамда кирувчи ва чиқувчи пакетларни фильтрлашга мослаштирилган, серверда ишловчи дастурдан фойдаланиш мумкин. Замонавий маршрутизаторлар ҳар бир порт билан бир неча ўнлаб қоидаларни боғлаши ва киришда, ҳам чиқишда пакетларни фильтрлаши мумкин.

Пакетли фильтрларнинг камчилиги сифатида қуйидагиларни кўрсатиш мумкин. Улар хавфсизликнинг юқори даражасини таъминламайди, чунки фақат пакет сарлавҳаларини текширадилар ва кўпгина керакли функцияларни мададламайди. Бу функцияларга, масалан, охирги узелларни аутентификациялаш, хабарлар пакетларини криптографик беркитиш, ҳамда уларнинг яхлитлигини ва ҳақиқийлигини текшириш киради. Пакетли фильтрлар дастлабки адресларни алмаштириб қўйиш ва хабарлар пакети таркибини рухсатсиз ўзгартириш каби кенг тарқалган тармоқ хужумларига заиф ҳисобланадилар. Бу хил брандмауэрларни "алдаш" қийин эмас - фильтрлашга рухсат берувчи қоидаларни қондирувчи пакет сарлавҳаларини шакллантириш кифоя.

Аммо, пакетли фильтрларнинг амалга оширилишининг соддалиги, юқори унумдорлиги, дастурий иловалар учун шаффофлиги ва нархининг

пастлиги, уларнинг ҳамма ерда тарқалишига ва тармоқ хавфсизлиги тизимининг мажбурий элементи каби ишлатилишига имкон яратди.

Сеанс сатҳи шлюзи, (*экранловчи транспорт* деб ҳам юритилади) виртуал уланишларни назоратлашга ва ташқи тармоқ билан ўзаро алоқа қилишда IP-адресларни трансляциялашга аталган. У OSI моделининг сеанс сатҳида ишлайди ва ишлаши жараёнида эталон моделнинг транспорт ва тармоқ сатҳларини ҳам қамраб олади. Сеанс сатҳи шлюзининг ҳимоялаш функциялари воситачилик функцияларига тааллуқли.

Виртуал уланишларнинг назорати алоқани квитирлашни кузатишдан ҳамда ўрнатилган виртуал каналлар бўйича ахборот узатилишининг назоратлашдан иборат. Алоқани квитирлашнинг назоратида сеанс сатҳида шлюз ички тармоқ ишчи станцияси ва ташқи тармоқ компьютери орасида виртуал уланишни кузатиб, сўралаётган алоқа сеансининг жоизлигини аниқлайди.

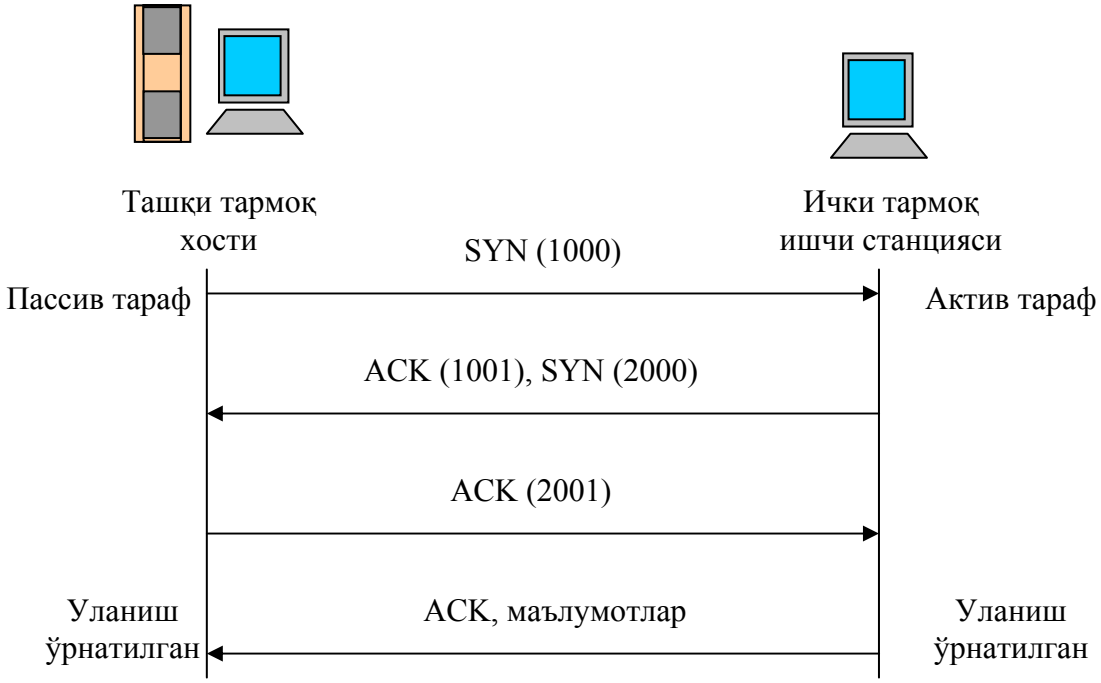
Бундай назорат TCP протоколининг сеанс сатҳи пакетларининг сарлавҳасидаги ахборотга асосланади. Аммо TCP-сарлавҳаларни тахлиллашда пакетли фильтр фақат манба ва қабул қилувчи портларининг номерини текширса, экранловчи транспорт алоқани квиртирлаш жараёнига тааллуқли бошқа ҳошияларни таҳлиллайди.

Алоқа сеансига сўровнинг жоизлигини аниқлаш учун сеанс сатҳи шлюзи қуйидаги ҳаракатларни бажаради. Ишчи станция (мижоз) ташқи тармоқ билан боғланишни сўраганида, шлюз бу сўровни қабул қилиб унинг фильтрлашнинг базавий мезонларни қаноатлантиришини, масалан сервер мижоз ва у билан ассоциацияланган исмнинг IP-адресини аниқлай олишини текширади. Сўнгра шлюз, мижоз исмидан ҳаракат қилиб, ташқи тармоқ компьютери билан уланишни ўрнатади ва TCP протоколи бўйича квитирлаш жараёнининг бажарилишини кузатади.

Бу муолажа SYN (Синхронлаш) ва ACK (Тасдиқлаш) байроқлари орқали белгиланувчи TCP-пакетларни алмашишдан иборат (7.7-расм).

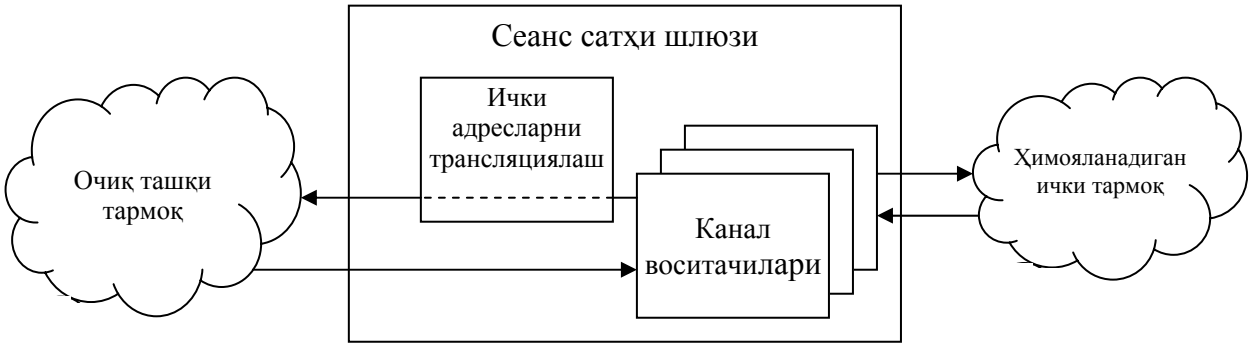
SYN байроқ билан белгиланган ва таркибида ихтиёрий сон, масалан 1000, бўлган TCP сеансининг биринчи пакети мижознинг сеанс очишга сўрови ҳисобланади. Бу пакетни олган ташқи тармоқ компьютери жавоб

тариқасида ACK байроқ билан белгиланган ва таркибида олинган пакетдагидан биттага катта (бизнинг ҳолда 1001) сон бўлган пакетни жўнатади. Шу тариқа, мижоздан SYN пакети олинганлиги тасдиқланади. Сўнгра, тескари муолажа амалга оширилади: ташқи тармоқ компьютери ҳам мижозга узатилувчи маълумотлар биринчи байтининг тартиб рақами билан (масалан, 2000) SYN пакетини жўнатади, мижоз эса уни олганлигини, таркибида 2001 сони бўлган пакетни узатиш орқали тасдиқлайди. Шу билан алоқани квиртирлаш жараёни тугалланади.



7.7–расм. TCP протоколи бўйича алоқани квитирлаш схемаси.

Сеанс сатҳи шлюзи (7.8-расм) учун сўралган сеанс жоиз ҳисобланади, қачонки алоқани квиртирлаш жараёни бажарилишида SYN ва ACK байроқлар, ҳамда TCP-пакетлари сарлавҳаларидаги сонлар ўзаро мантиқий боғланган бўлса.



7.8-расм. Сеанс сатҳи шлюзи ишлаш схемаси

Ички тармоқнинг ички станцияси ва ташқи тармоқнинг компьютери TCP сеансининг авторизацияланган қатнашчилари эканлиги ҳамда ушбу сеанснинг жоизлиги тасдиқланганидан сўнг шлюз уланишни ўрнатади. Бунда шлюз уланишларининг махсус жадвалига мос ахборотни (жўнатувчи ва қабул қилувчи адреслари, уланиш ҳолати, кетма-кетлик номери хусусидаги ахборот ва ҳ.) киритади.

Шу ондан бошлаб шлюз пакетларни нусхалайди ва иккала томонга йўналтириб, ўрнатилган виртуал канал бўйича ахборот узатилишини назорат қилади. Ушбу назорат жараёнида сеанс сатҳи шлюзи пакетларни фильтрламайди. Аммо у узатилувчи ахборот сонини назорат қилиши ва қандайдир чегарадан ошганида уланишни узиши мумкин. Бу эса, ўз навбатида, ахборотнинг рухсатсиз экспорт қилинишига тўсиқ бўлади. Виртуал уланишлар хусусидаги қайдлаш ахборотининг тўпланиши ҳам мумкин.

Сеанс сатҳи шлюзларида виртуал уланишларни назоратлашда *канал воситачилари* (pipe proxy) деб юритилувчи махсус дастурлардан фойдаланилади. Бу воситачилар ички ва ташқи тармоқлар орасида виртуал каналларни ўрнатади, сўнгра TCP/IP иловалари генерациялаган пакетларнинг ушбу канал орқали узатилишини назоратлайди.

Канал воситачилари TCP/IPнинг муайян хизматларига мўлжалланган. Шу сабабли ишлаши муайян иловаларнинг воситачи-дастурларига асосланган татбиқий сатҳ шлюзлари имкониятларини кенгайтиришда сеанс сатҳ шлюзларидан фойдаланиш мумкин.

Сеанс сатҳи шлюзи ташқи тармоқ билан ўзаро алоқада тармоқ сатҳи ички адресларини (IP-адресларини) трансляциялашни ҳам таъминлайди. Ички адресларни трансляциялаш ички тармоқдан ташқи тармоққа жўнатилувчи барча пакетларга нисбатан бажарилади.

Амалга оширилиши нуқтаи назаридан сеанс сатҳи шлюзи етарлича оддий ва нисбатан ишончли дастур ҳисобланади. У экранловчи маршрутизаторни виртуал уланишларни назоратлаш ва ички IP-адресларни трансляциялаш функциялари билан тўлдиради.

Сеанс сатҳи шлюзининг камчиликлари – экранловчи маршрутизаторларнинг камчиликларига ўхшаш. Ушбу технологиянинг яна бир жиддий

камчилиги маълумотлар ҳошиялари таркибини назоратлаш мумкин эмаслиги. Натижада, нияти бузуқ одамларга зарар келтирувчи дастурларни ҳимояланувчи тармоққа узатиш имконияти туғилади. Ундан ташқари, TCP-сессиясининг (TCP hijacking) ушлаб қолинишида нияти бузуқ одам хужумларини ҳатто рухсат берилган сессия доирасида амалга ошириши мумкин.

Амалда аксарият сеанс сатҳ шлюзлари мустақил маҳсулот бўлмай, татбиқий сатҳ шлюзлари билан комплектда тақдим этилади.

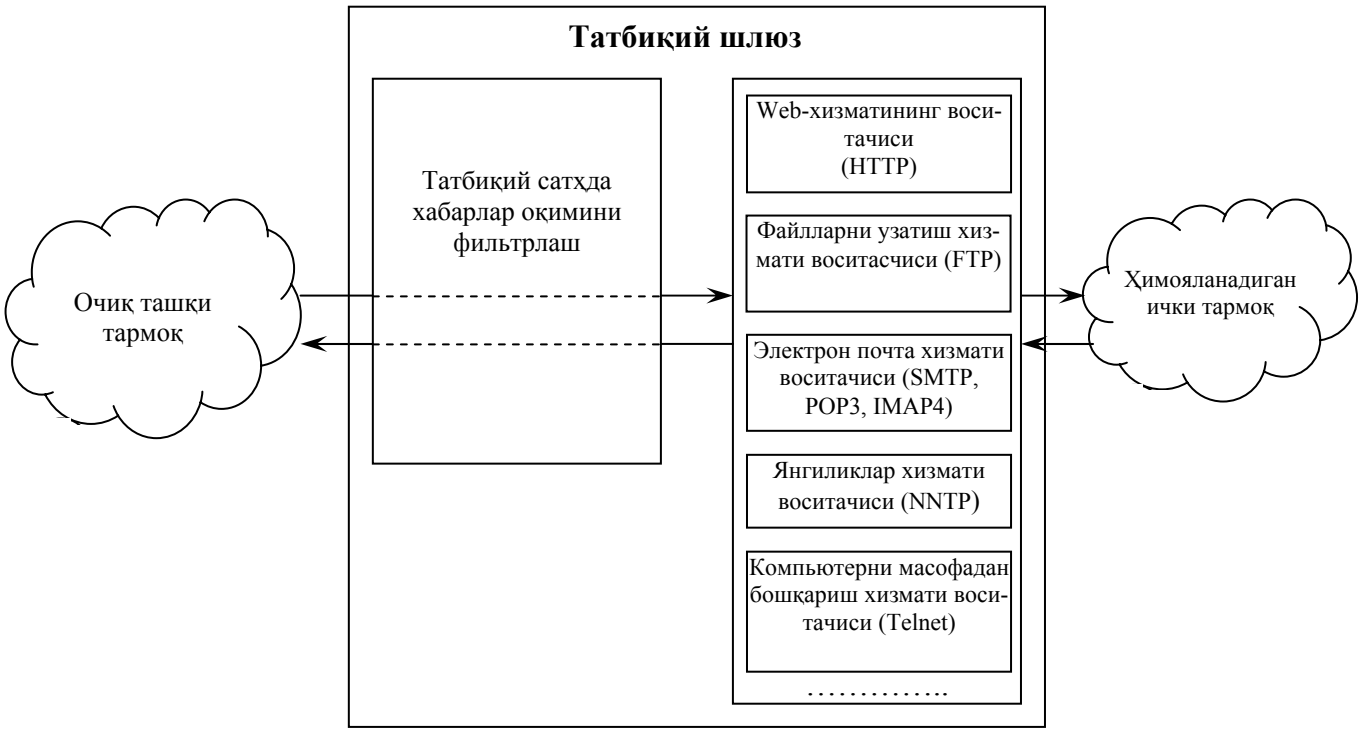
Татбиқий сатҳ шлюзи (*экранловчи шлюз* деб ҳам юритилади) OSI моделининг татбиқий сатҳида ишлаб, тақдимий сатҳни ҳам қамраб олади ва тармоқлараро алоқанинг энг ишончли ҳимоясини таъминлайди. Татбиқий сатҳ шлюзининг ҳимоялаш функциялари, сеанс сатҳи шлюзига ўхшаб, воситачилик функцияларига тааллуқли. Аммо, татбиқий сатҳ шлюзи сеанс сатҳи шлюзига қараганда ҳимоялашнинг анча кўп функцияларини бажариши мумкин:

- брандмауэр орқали уланишни ўрнатишга уринишда фойдаланувчиларни идентификациялаш ва аутентификациялаш;
- шлюз орқали узатилувчи ахборотнинг ҳақиқийлигини текшириш;
- ички ва ташқи тармоқ ресурсларидан фойдаланишни чегаралаш;
- ахборотлар оқимини фильтрлаш ва ўзгартириш, масалан, вирусларни динамик тарзда қидириш ва ахборотни шаффоф шифрлаш;
- ходисаларни қайдлаш, ходисаларга реакция кўрсатиш, ҳамда қайдланган ахборотни тахлиллаш ва хисоботларни генерациялаш;
- ташқи тармоқдан сўралувчи маълумотларни кэшлаш.

Татбиқий сатҳ шлюзи функциялари воситачилик функцияларига тааллуқли бўлганлиги сабабли, бу шлюз универсал компьютер ҳисобланади ва бу компьютерда ҳар бир хизмат кўрсатилувчи татбиқий протокол (HTTP, FTP, SMTP, NNTP ва ҳ.) учун биттадан воситачи дастур (экранловчи агент) ишлатилади. TCP/IPнинг ҳар бир хизматининг воситачи дастури (application proxy) айнан шу хизматга тааллуқли хабарларни ишлашга ва ҳимоялаш функцияларини бажаришга мўлжалланган.

Татбиқий сатҳ шлюзи мос экранловчи агентлар ёрдамида кирувчи ва чиқувчи пакетларни ушлаб қолади, ахборотни нусхалайди ва қайта

жўнатади, яъни ички ва ташқи тармоқлар орасидаги тўғридан-тўғри уланишни истисно қилган ҳолда, сервер-воситачи функциясини бажаради (7.9-расм).



7.9-расм. Татбиқий шлюз ишлаш схемаси.

Татбиқий сатҳ шлюзи ишлатадиган воситачилар сеанс сатҳи шлюзларининг канал воситачиларидан жиддий фарқланади. Биринчидан, татбиқий сатҳ шлюзлари муайян иловалар (дастурий серверлар) билан боғланган, иккинчидан улар OSI моделининг татбиқий сатҳида хабарлар оқимини фильтрлашлари мумкин.

Татбиқий сатҳ шлюзлари воситачи сифатида мана шу мақсадлар учун махсус ишлаб чиқилган TCP/IPнинг муайян хизматларининг дастурий серверлари – HTTP, FTP, SMTP, NNTP ва ҳ. – серверларидан фойдаланади. Бу дастурий серверлар брандмауэрларда резидент режимида ишлайди ва TCP/IPнинг мос хизматларига тааллуқли ҳимоялаш функцияларини амалга оширади. UDP трафигига UDP-пакетлар таркибининг махсус транслятори хизмат кўрсатади.

Ички тармоқ ишчи сервери ва ташқи тармоқ компьютери орасида иккита уланиш амалга оширилади: ишчи станциядан брандмауэргача ва брандмауэрдан белгиланган жойгача. Канал воситачиларидан фарқли ҳолда,

татбиқий сатҳ шлюзининг воситачилари фақат ўзлари хизмат қилувчи иловалар генерациялаган пакетларни ўтказади. Масалан, HTTP хизматининг воситачи-дастури фақат шу хизмат генерациялаган трафикни ишлайди.

Агар қандайдир иловада ўзининг воситачиси бўлмаса, татбиқий сатҳдаги шлюз бундай иловани ишлай олмайди ва у блокировка қилинади. Масалан, агар татбиқий сатҳдаги шлюз фақат HTTP, FTP ва Telnet воситачи-дастурларидан фойдаланса, у фақат шу хизматларга тегишли пакетларни ишлайди ва қолган хизматларнинг пакетларини блокировка қилади.

Татбиқий сатҳ шлюзи воситачилари, канал воситачиларидан фарқли ҳолда, ишланувчи маълумотлар таркибини текширишни таъминлайди. Улар ўзлари хизмат кўрсатадиган татбиқий сатҳ протоколларидаги командаларнинг алоҳида хилларини ва хабарлардаги ахборотлани фильтрлашлари мумкин.

Татбиқий сатҳ шлюзини созлашда ва хабарларни фильтрлаш қоидаларини тавсифлашда қуйидаги параметрлардан фойдаланилади: сервис номи, ундан фойдаланишнинг жоиз вақт оралиғи, ушбу сервисга боғлиқ хабар таркибига чегаралашлар, сервис ишлатадиган компьютерлар, фойдаланувчи идентификатори, аутентификациялаш схемалари ва ҳ.

Татбиқий сатҳ шлюзи қуйидаги афзалликларга эга:

- аксарият воситачилик функцияларини бажара олиши туфайли локал тармоқ ҳимоясининг юқори даражасини таъминлайди;

- иловалар сатҳида ҳимоялаш кўпгина қўшимча текширишларни амалга оширишга имкон беради, натижада дастурий таъминот камчиликларига асосланган муваффақиятли хужумлар ўтказиш эҳтимоллиги камаяди;

- татбиқий сатҳ шлюзининг ишга лаёқатлиги бузилса, бўлинувчи тармоқлар орасида пакетларнинг тўппа-тўғри ўтиши блокировка қилинади, натижада, рад қилиниши туфайли ҳимояланувчи тармоқнинг хавфсизлиги пасаймайди.

Татбиқий сатҳ шлюзининг камчиликларига қуйидагилар киради:

- нархининг нисбатан юқорилиги;

- брандмауэрнинг ўзи, ҳамда уни ўрнатиш ва конфигурациялаш муолажаси етарлича мураккаб;

- компьютер платформаси унумдорлигига ва ресурслари ҳажмига қуйиладиган талабларнинг юқорилиги;

- фойдаланувчилар учун шаффофликнинг йўқлиги ва тармоқлараро алоқа ўрнатилишида ўтказиш қобилиятининг сусайиши.

Охирги камчиликка батафсил тухталамиз. Воситачилар сервер ва мижоз орасида пакетлар узатилишида оралиқ ролини бажаради. Аввал воситачи билан уланиш ўрнатилади, сўнгра воситачи адресат билан уланишни яратиш ёки яратмаслик хусусида қарор қабул қилади. Мос ҳолда татбиқий сатҳ шлюзи ишлаши жараёнида ҳар қандай рухсат этилган уланишни қайталайди. Натижада фойдаланувчилар учун шаффофлик йўқолади ва уланишга хизмат қилишга қўшимча ҳаражат сарфланади.

Эксперт сатҳи шлюзи. Татбиқий сатҳ шлюзининг фойдаланувчилар учун шаффофлигининг йўқлиги ва тармоқлараро алоқа ўрнатилишида ўтказиш қобилиятининг сусайиши каби жиддий камчиликларини бартараф этиш мақсадида пакетларни фильтрлашнинг янги технологияси ишлаб чиқилган. Бу технологияни баъзида *уланиш холатини назоратлашли фильтрлаш* (stateful inspection) ёки эксперт сатҳидаги фильтрлаш деб юритишади. Бундай фильтрлаш пакетлар ҳолатини кўп сатҳли таҳлиллашнинг махсус усуллари (SMLT) асосида амалга оширилади.

Ушбу гибрид технология тармоқ сатҳида пакетларни ушлаб қолиш ва ундан уланишни назорат қилишда ишлатилувчи татбиқий сатҳ ахборотини чиқариб олиш орқали уланиш ҳолатини кузатишга имкон беради.

Ишлаши асосини ушбу технология ташкил этувчи тармоқлараро экран *эксперт сатҳ брандмауэри* деб юритилади. Бундай брандмауэрлар ўзида экранловчи маршрутизаторлар ва татбиқий сатҳ шлюзлари элементларини уйғунлаштиради. Улар ҳар бир пакет таркибини берилган хавфсизлик сиёсатига мувофиқ баҳолайдилар.

Шундай қилиб эксперт сатҳидаги брандмауэрлар қуйидагиларни назоратлашга имкон беради:

- мавжуд қоидалар жадвали асосида ҳар бир узатилувчи пакетни;

- ҳолатлар жадвали асосида ҳар бир сессияни;

- ишлаб чиқилган воситачилар асосида ҳар бир иловани.

Эксперт сатҳ тармоқлараро экранларининг афзалликлари сифатида уларнинг фойдаланувчилар учун шаффофлигини, ахборот оқимини ишлашининг юқори тезкорлигини ҳамда улар орқали ўтувчи пакетларнинг IP-адресларини ўзгартирмаслигини кўрсатиш мумкин. Охирги афазаллик. IP-адресдан фойдаланувчи татбиқий сатҳнинг ҳар қандай протоколининг бундай брандмауэрлардан ҳеч қандай ўзгаришсиз ёки махсус дастурлашсиз бирга ишлай олишини англатади.

Бундай брандмауэрларнинг авторизацияланган мижоз ва ташқи тармоқ компьютери орасида тўғридан-тўғри уланишга йўл қўйиши, ҳимоянинг унчалик юқори бўлмаган даражасини таъминлайди. Шу сабабли амалда эксперт сатҳини фильтрлаш технологиясидан комплекс брандмауэрлар ишлаши самарадорлигини оширишда фойдаланилади. Эксперт сатҳнинг фильтрлаш технологиясини ишлатувчи комплекс брандмауэрларга мисол тариқасида Fire Wall-1 ва ON Guardларни кўрсатиш мумкин.

7.3. Тармоқлараро экранлар асосидаги тармоқ ҳимоясининг схемалари

Тармоқлараро алоқани самарали ҳимоялаш учун брандмауэр тизими тўғри ўрнатилиши ва конфигурацияланиши лозим. Ушбу жараён қуйидагиларни ўз ичига олади:

- тармоқлараро алоқа сиёсатини шакллантириш;
- брандмауэрни улаш схемасини танлаш ва параметрларини созлаш.

Тармоқлараро алоқа сиёсатини шакллантириш

Тармоқлараро алоқа сиёсатини шакллантиришда қуйидагиларни аниқлаш лозим:

- тармоқ сервисларидан фойдаланиш сиёсати;
- тармоқлараро экран ишлаши сиёсати.

Тармоқ сервисларидан фойдаланиш сиёсати ҳимояланувчи компьютер тармоқнинг барча сервисларини тақдим этиш, ҳамда улардан фойдаланиш қоидаларини белгилайди. Ушбу сиёсат доирасида тармоқ экрани орқали тақдим этилувчи барча сервислар ва ҳар бир сервис учун мижозларнинг жоиз адреслари берилиши лозим. Ундан ташқари, фойдаланувчилар учун

қачон ва қайси фойдаланувчилар қайси сервисдан ва қайси компьютерда фойдаланишларини тавсифловчи қоидалар кўрсатилиши лозим. Фойдаланиш усулларига чегаралашлар ҳам берилади. Бу чегаралашлар фойдаланувчиларнинг Internetнинг ман этилган сервисларидан айланма йўл орқали фойдаланишларига йўл қўймаслик учун зарур. Фойдаланувчилар ва компьютерларни аутентификациялаш қоидалари, ҳамда ташкилот локал тармоғи ташқарисидаги фойдаланувчиларнинг ишлаш шароитлари алоҳида белгиланиши лозим.

Тармоқлараро экран ишлаши сиёсатида тармоқлараро алоқани бошқаришнинг брандмауэр ишлаши асосидаги базавий принципи берилади. Бундай принципларнинг қуйидаги иккитасидан бири танланиши мумкин:

- ошкора рухсат этилмагани ман қилинган;
- ошкора ман этилмаганига рухсат берилган.

"Ошкора рухсат этилмагани ман қилинган" принципи танланганида тармоқлараро экран шундай созланадики, ҳарқандай рухсат этилмаган тармоқлараро алоқалар блокировка қилинади. Ушбу принцип ахборот хавфсизлигининг барча соҳаларида ишлатилувчи фойдаланишнинг мумтоз моделига мос келади. Бундай ёндашиш, имтиёзларни минималлаштириш принципини адекват амалга оширишга имкон бериши сабабли, хавфсизлик нуқтаи назаридан яхшироқ ҳисобланади. Моҳияти бўйича "ошкора рухсат этилмагани ман қилинган" принципи билмаслик зарар келтириши фактини эътироф этишдир. Таъкидлаш лозимки, ушбу принципга асосан таърифланган фойдаланиш қоидалари фойдаланувчиларга маълум ноқулайликлар туғдириши мумкин.

"Ошкора ман этилмаганига рухсат берилган" принципи танланганида тармоқлараро экран шундай созланадики, фақат ошкора ман этилган тармоқлараро алоқалар блокировка қилинади. Бу ҳолда, фойдаланувчилар томонидан тармоқ сервисларидан фойдаланиш қулайлиги ошади, аммо тармоқлараро алоқа хавфсизлиги пасаяди. Фойдаланувчиларнинг тармоқлараро экранни четлаб ўтишларига имкон туғилади, масалан улар сиёсат ман қилмаган (ҳатто сиёсатда кўрсатилмаган) янги сервисларидан фойдаланишлари мумкин. Ушбу принцип амалга оширилишида ички

тармоқ хакерларнинг хужумларидан камроқ ҳимояланган бўлади. Шу сабабли, тармоқлараро экранларни ишлаб чиқарувчилари одатда ушбу принципдан фойдаланмайдилар.

Тармоқлараро экран симметрик эмас. Унга ички тармоқнинг ташқи тармоқдан ва аксинча фойдаланишни чегараловчи қоидалар алоҳида берилади. Умумий ҳолда, тармоқлараро экраннинг иши қуйидаги иккита гуруҳ функцияларни динамик тарзда бажаришга асосланган:

- у орқали ўтаётган ахборот оқимини фильтрлаш;
- тармоқлараро алоқа амалга оширилишида воситачилик.

Оддий тармоқлараро экранлар бу функцияларнинг бирини бажаришга мўлжалланган. Комплекс тармоқлараро экранлар ҳимоялашнинг кўрсатилган функцияларининг биргаликда бажарилишини таъминлайди.

Тармоқлараро экранларни улашнинг асосий схемалари. Корпоратив тармоқни глобал тармоқларга улаганда ҳимояланувчи тармоқнинг глобал тармоқдан ва глобал тармоқнинг ҳимояланувчи тармоқдан фойдаланишини чегаралаш, ҳамда уланувчи тармоқдан глобал тармоқнинг масофадан рухсатсиз фойдаланишидан ҳимоялашни таъминлаш лозим. Бунда ташкилот ўзининг тармоғи ва унинг компонентлари хусусидаги ахборотни глобал тармоқ фойдаланувчиларидан беркитишга манфаатдор. Масофадаги фойдаланувчилар билан ишлаш ҳимояланувчи тармоқ ресурсларидан фойдаланишнинг қатъий чегараланишини талаб этади.

Ташкилотдаги корпоратив тармоқ таркибида кўпинча ҳимояланишнинг турли сатҳли бирнечи сегментларга эга бўлиши эҳтиёжи туғилади:

- бемалол фойдаланилувчи сегментлар (масалан, реклама WWW-серверлари);
- фойдаланиш чегараланган сегментлар (масалан, ташкилотнинг масофадаги узеллари ходимларининг фойдаланиши учун);
- ёпиқ сегментлар (масалан, ташкилотнинг молия локал қисм тармоғи)

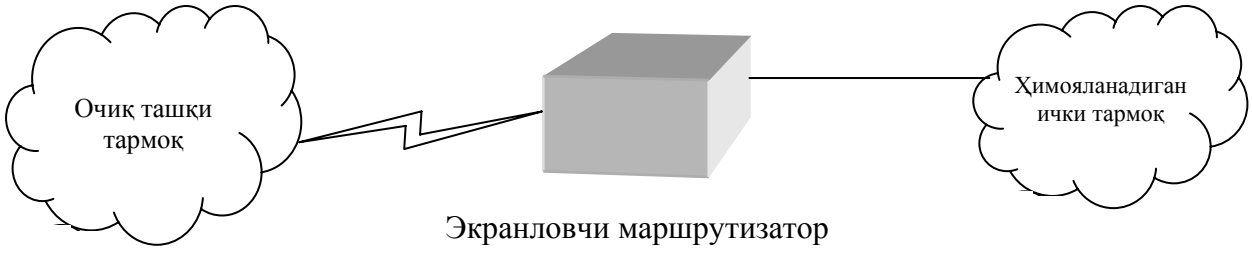
Тармоқлараро экранларни улашда турли схемалардан фойдаланиш мумкин. Бу схемалар ҳимояланувчи тармоқ ишлаши шароитига, ҳамда иш-

латиладиган брандмауэрларнинг тармоқ интерфейслари сонига ва бошқа характеристикаларига боғлиқ. Тармоқлараро экранни улашнинг қуйидаги схемалари кенг тарқалган:

- экранловчи маршрутизатордан фойдаланилган ҳимоя схемалари;
- локал тармоқни умумий ҳимоялаш схемалари;
- ҳимояланувчи ёпиқ ва ҳимояланмайдиган очиқ кисм тармоқли схемалар;
- ёпиқ ва очиқ қисм тармоқларни алоҳида ҳимояловчи схемалар.

Экранловчи маршрутизатордан фойдаланилган ҳимоя схемаси.

Пакетларни фильтрлашга асосланган тармоқлараро экран кенг тарқалган ва амалга оширилиши осон. У ҳимояланувчи тармоқ ва бўлиши мумкин бўлган ғаним очиқ тармоқ орасида жойлашган экранловчи маршрутизатордан иборат (7.10-расм).



7.10-расм. Тармоқлараро экран – экранловчи маршрутизатор

Экранловчи маршрутизатор (пакетли фильтр) кирувчи ва чиқувчи пакетларни уларнинг адреслари ва портлари асосида блокировка қилиш ва фильтрлаш учун конфигурацияланган.

Ҳимояланувчи тармоқдаги компьютерлар Internetдан тўғридан-тўғри фойдаланаолади, Internetнинг улардан фойдаланишининг кўп қисми эса блокировка қилинади. Умуман, экранловчи маршрутизатор юқорида тавсифланган ҳимоялаш сиёсатидан исталганини амалга ошириши мумкин. Аммо, агар маршрутизатор пакетларни манба порти ва кириш йўли ва чиқиш йўли портлари номери бўйича фильтрламаса, "ошкора рухсат этилмагани ман қилинган" сиёсатини амалга ошириш қийинлашади.

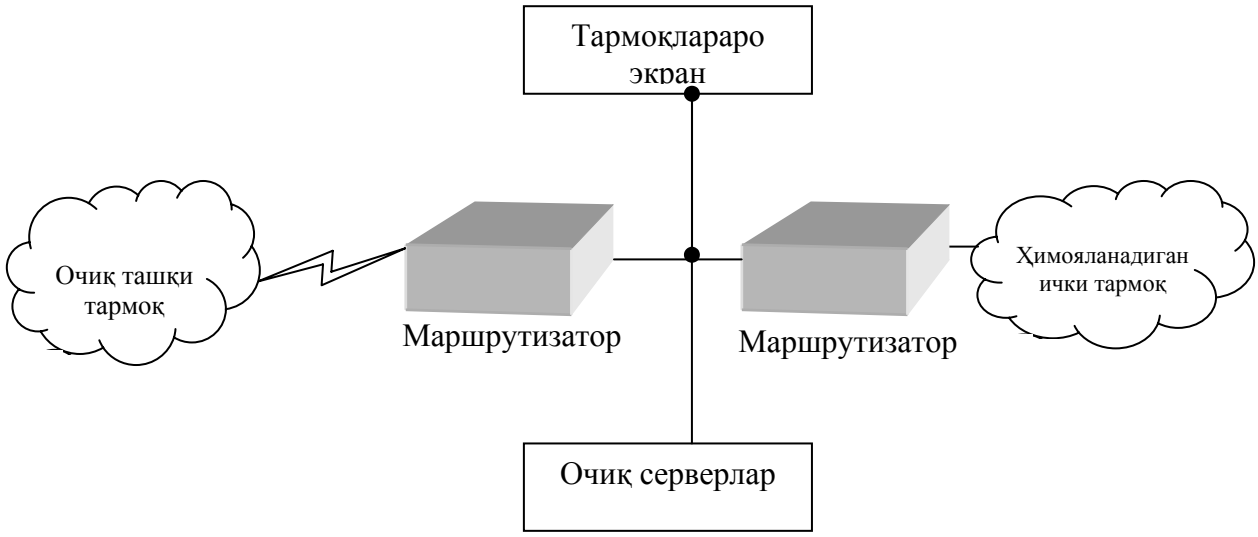
Пакетларни фильтрлашга асосланган тармоқлараро экраннинг камчиликлари қуйидагилар:

- фильтрлаш қоидаларининг мураккаблиги; баъзи ҳолларда бу қоидалар мажмуи бажарилмаслиги мумкин;

- фильтрлаш қоидаларини тўлиқ тестлаш мумкин эмаслиги; бу тармоқни тестланмаган хужумлардан ҳимояланмаслигига олиб келади;

- ходисаларни руйхатга олиш имкониятининг йўқлиги; натижада маъмурга машрутизаторнинг хужумга дуч келганлигини ва обрўсизлантирилганлигини аниқлаш қийинлашади.

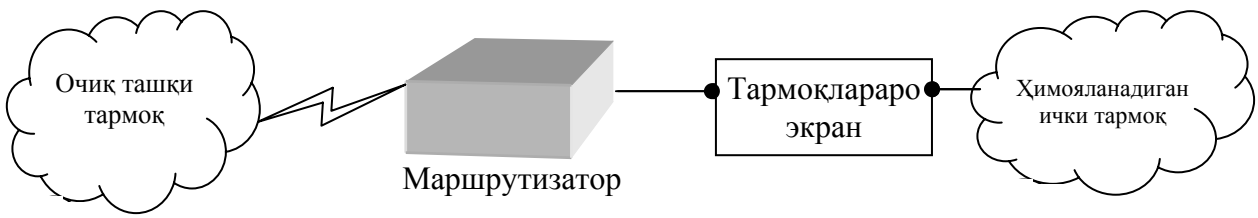
Локал тармоқни умумий ҳимоялаш схемалари. Битта тармоқ интерфейсли брандмауэрлардан фойдаланилган ҳимоялаш схемалари (7.11-расм)



7.11-расм. Битта тармоқ интерфейсли firewall ёрдамида локал тармоқни ҳимоялаш

хавфсизлик ва конфигурациялашнинг қулайлиги нуқтаи назаридан самарасиз ҳисобланади. Улар ички ва ташқи тармоқларни физик ажратмайдилар, демак, тармоқлараро алоқанинг ишончли ҳимоясини таъминлай олмайдилар.

Локал тармоқни умумий ҳимоялаш схемаси энг оддий ечим бўлиб, унда брандмауэр локал тармоқни ташқи ғаним тармоқдан бутунлай экранлайди (7.12-расм). Маршрутизатор ва брандмауэр орасида фақат битта йўл



7.12-расм. Локал тармоқни умумий ҳимоялаш схемаси

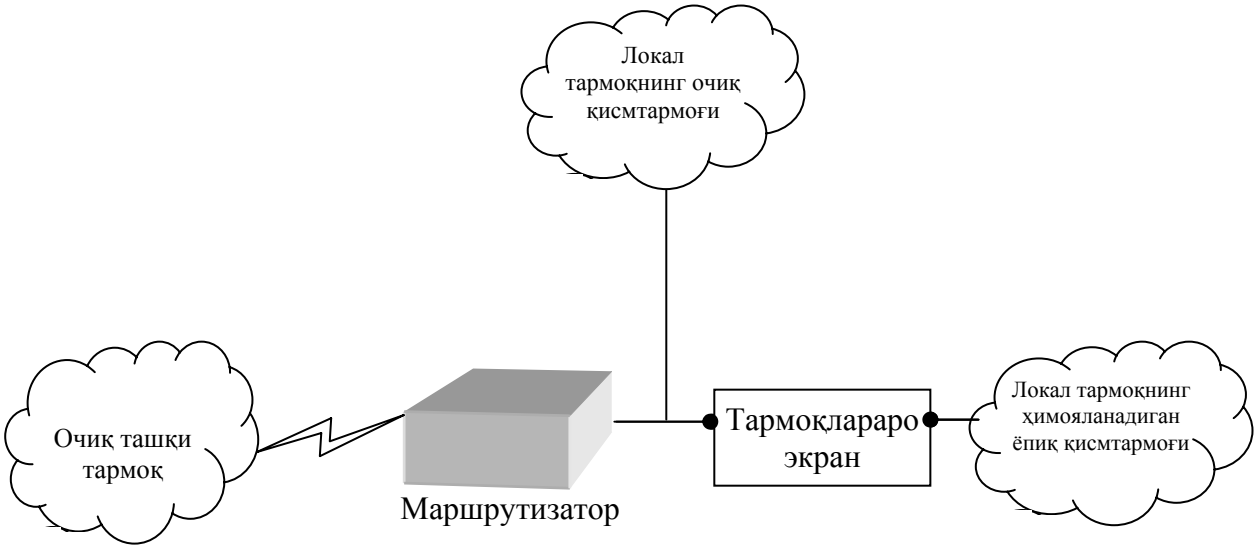
бўлиб, бу йўл орқали бутун трафик ўтади. Брандмауэрнинг ушбу варианти "ошкора рухсат этилмагани ман қилинган" принципига асосланган ҳимоялаш сиёсатини амалга оширади. Одатда маршрутизатор шундай созланадики, брандмауэр ташқаридан кўринадиган ягона машина бўлади.

Локал тармоқ таркибидаги очиқ серверлар ҳам тармоқлараро экранлар томонидан ҳимояланади. Аммо, ташқи тармоқ фойдаланаоладиган серверларни ҳимояланувчи локал тармоқларнинг бошқа ресурслари билан бирлаштириш тармоқлараро алоқа хавфсизлигини жиддий пасайтиради.

Тармоқлараро экран фойдаланадиган хостга фойдаланувчиларни кучайтирилган аутентификациялаш учун дастур ўранатилиши мумкин.

Ҳимояланувчи ёпиқ ва ҳимояланмайдиган очиқ қисм тармоқли схемалар. Агар локал тармоқ таркибида умумфойдаланувчи очиқ серверлар бўлса уларни тармоқлараро экрандан олдин очиқ қисм тармоқ сифатида чиқариш мақсадга мувофиқ ҳисобланади (7.13-расм).

Ушбу усул локал тармоқ ёпиқ қисмининг кучли ҳимояланишини, аммо тармоқлараро экрангача жойлашган очиқ серверларнинг пасайган ҳимояланишини таъминлайди.

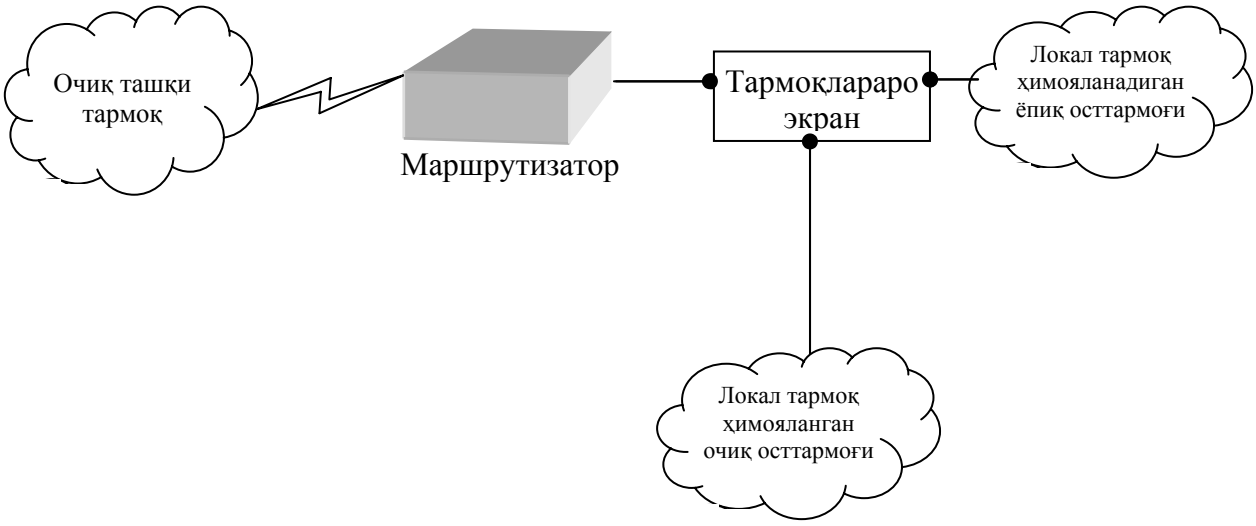


7.13-расм. Ҳимояланадиган ёпиқ ва ҳимояланмайдиган очиқ қисмтармоқли схема

Баъзи брандмауэрлар бу серверларни ўзида жойлаштиради. Аммо бу брандмауэрнинг хавфсизлиги ва компьютернинг юкланиши нуқтаи назаридан яхши ечим ҳисобланмайди. Ҳимояланувчи ёпиқ ва ҳимояланмайдиган очиқ қисм тармоқли схемани очиқ қисм тармоқ хавфсизлигига қўйиладиган

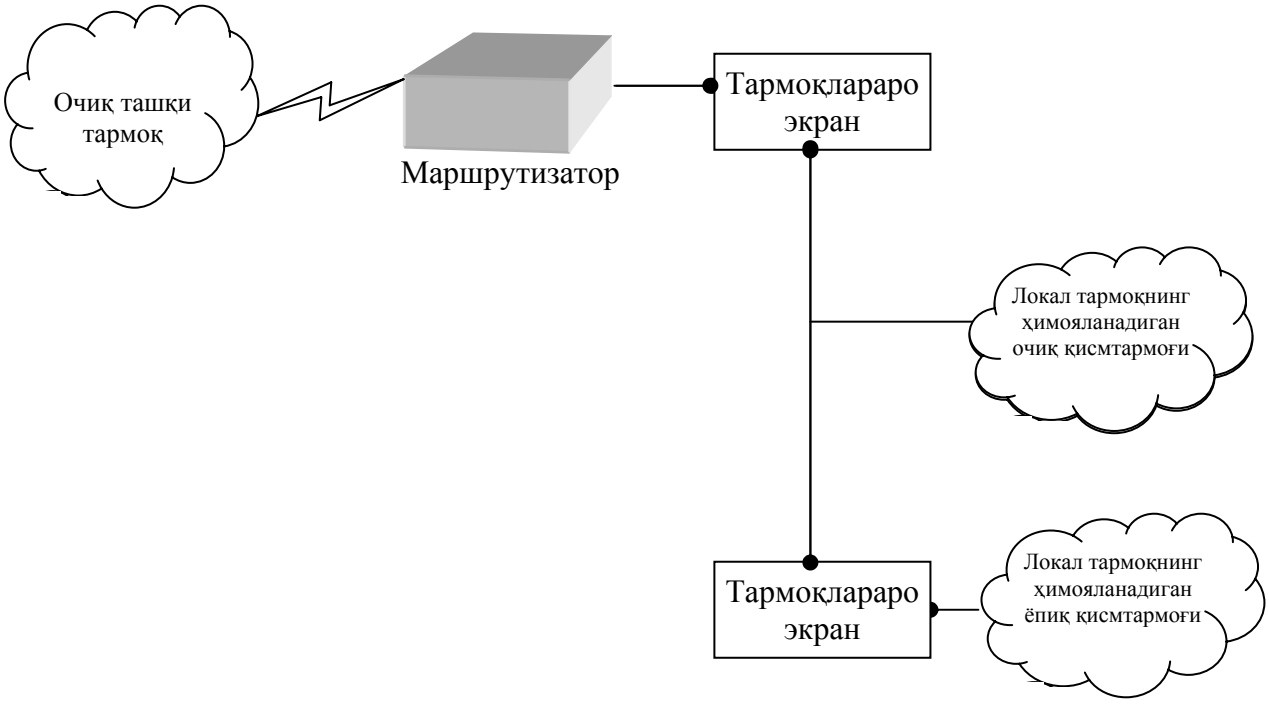
талабларнинг бўлмаган ҳолларида ишлатилиши мақсадга мувофиқ ҳисобланади. Агар очиқ сервер хавфсизлигига юқори талаблар қўйилса, ёпиқ ва очиқ қисм тармоқларни алоҳида ҳимоялаш схемаларидан фойдаланиш зарур.

Ёпиқ ва очиқ қисм тармоқларни алоҳида ҳимояловчи схемалар. Бундай схемалар учта тармоқ интерфейсли битта брандмауэр (7.14-расм)



7.14 -расм. Учта тармоқ интерфейсли бир брандмауэр асосида ёпиқ ва очиқ қисм тармоқларни алоҳида ҳимоялаш схемаси

ёки иккита тармоқ интерфейсли иккита брандмауэр (7.15-расм) асосида



7.15-расм. Иккита тармоқ интерфейсли иккита брандмауэр асосида ёпиқ ва очиқ қисмтармоқларни алоҳида ҳимоялаш схемаси

қурилиши мумкин. Иккала ҳолда ҳам очиқ ва ёпиқ қисм тармоқлардан фақат тармоқлараро экран орқали фойдаланиш мумкин. Бунда очиқ қисм тармоқдан фойдаланиш ёпиқ қисм тармоқдан фойдаланишга имкон бермайди.

Иккита брандмауэрли схема тармоқлараро алоқа хавфсизлигининг юқори даражасини таъминлайди. Бунда ҳар бир брандмауэр ёпиқ тармоқни ҳимоялашнинг алоҳида эшелонини ҳосил қилади, ҳимояланувчи очиқ қисм тармоқ эса экранловчи қисм тармоқ сифатида иштирок этади.

Одатда экранловчи қисм тармоқ шундай конфигурацияланадики, қисм тармоқ компьютеридан ғаним ташқи тармоқ ва локал тармоқнинг ёпиқ қисм тармоғи фойдалана олсин. Аммо ташқи тармоқ ва ёпиқ қисм тармоқ орасида тўғридан-тўғри ахборот пакетларини алмашиш мумкин эмас. Экранловчи қисм тармоқли тизимни хужум қилишда, бўлмаганида ҳимоянинг иккита мустақил чизиғини босиб ўтишга тўғри келади. Бу эса жуда мураккаб масала ҳисобланади. Тармоқлараро экран ҳолатларини мониторинглаш воситалари бундай уринишни доимо аниқлаши ва тизим маъмури ўз вақтида рухсатсиз фойдаланишга қарши зарурий чоралар кўриши мумкин.

Таъкидлаш лозимки, алоқанинг коммутацияланувчи линияси орқали уланувчи масофадаги фойдаланувчиларнинг иши ҳам ташкилотда ўтказилувчи хавфсизлик сиёсатига мувофиқ назорат қилиниши шарт. Бундай масаланинг намунавий ҳал этилиши – зарурий функционал имкониятларга эга бўлган масофадан фойдаланиш серверини (терминал серверни) ўрнатиш. Терминал сервер бир неча асинхрон портларга ва локал тармоқнинг битта интерфейсига эга бўлган тизим ҳисобланади. Асинхрон портлар ва локал тармоқ орасида ахборот алмашиш фақат ташқи фойдаланувчини аутентификациялашдан кейин амалга оширилади.

Терминал серверни улаш шундай амалга ошириш лозимки, унинг иши фақат тармоқлараро экран орқали бажарилсин. Бу масофалаги фойдаланувчиларнинг ташкилот ахборот ресурслари билан ишлаш хавфсизлигининг керакли даражасини таъминлашга имкон беради.

Терминал серверни очиқ кисм тармоқ таркибига киритилганида бундай уланиш жоиз ҳисобланади. Терминал сервернинг дастурий таъминоти

коммутацияланувчи каналлар орқали алоқа сеансларини маъмурлаш ва назоратлаш имкониятини таъминлаши лозим. Замонавий терминал серверларни бошқариш модуллари серверни ўзини хавфсизлигини таъминлаш ва мижозларнинг фойдаланишини чегаралаш бўйича етарлича ривожланган имкониятларга эга ва қуйидаги функцияларни бажаради:

- кетма-кет портлардан, PPP протоколи бўйича масофадан, ҳамда маъмур консолидан фойдаланишда локал паролни ишлатиш;

- локал тармоқнинг қандайдир машинасининг аутентификациялашга сўровидан фойдаланиш;

- аутентификациялашнинг ташқи воситаларидан фойдаланиш;

- терминал сервери портларидан фойдаланишни назоратловчи руйхатни ўрнатиш;

- терминал сервер орқали алоқа сеансларини протоколлаш.

Шахсий ва тақсимланган тармоқ экранлари. Охирги бир неча йил мобайнида корпоратив тармоқ тузилмасида маълум ўзгаришлар содир бўлди. Агар илгари бундай тармоқ чегараларини аниқ белгилаш мумкин бўлган бўлса, ҳозирда бу мумкин эмас. Яқиндаёқ бундай чегара барча маршрутизаторлар ёки бошқа қурилмалар (масалан, модемлар) орқали ўтар ва улар ёрдамида ташқи тармоқларга чиқилар эди. Аммо ҳозирда тармоқлараро экран орқали ҳимояланувчи тармоқнинг тўла ҳуқуқли эгаси – ҳимояланувчи периметр ташқарисидаги ходим ҳисобланади. Бундай ходимлар сирасига уйдаги ёки меҳнат сафаридаги ходимлар киради. Шубхасиз, уларга ҳам ҳимоя зарур. Аммо барча анъанавий тармоқлараро экранлар шундай қурилганки, ҳимояланувчи фойдаланувчилар ва ресурслар уларнинг ҳимоясида корпоратив ёки локал тармоқнинг ички томонида бўлишлари шарт. Бу эса мобил фойдаланувчилар учун мумкин эмас.

Бу муаммони ечиш учун қуйидаги ёндашишлар таклиф этилган:

- тақсимланган тармоқлараро экранлардан (distributed firewall) фойдаланиш;

- виртуал хусусий тармоқ VPNлар имкониятидан фойдаланиш.

Тақсимланган тармоқлараро экран тармоқнинг алоҳида компьютерини ҳимояловчи марказдан бошқарилувчи тармоқ мини-экранлар мажмуидир.

Тақсимланган брандмауэрларнинг қатор функциялари (масалан марказдан бошқариш, хавфсизлик сиёсатини тарқатиш) шахсий фойдаланувчилар учун ортиқча бўлганлиги сабабли, тақсимланган брандмауэрлар модификацияланди. Янги ёндашиш *шахсий тармоқли экранлаш технологияси* номини олди. Бунда тармоқли экран ҳимояланувчи шахсий компьютерда ўрнатилади. Компьютернинг шахсий экрани (personal firewall) ёки тармоқли экранлаш тизими деб аталувчи бундай экран, бошқа барча тизимли ҳимоялаш воситаларига боғлиқ бўлмаган ҳолда бутун чиқувчи ва кирувчи трафикни назоратлайди. Алоҳида компьютерни экранлашда тармоқ сервисдан фойдаланувчанлик мададланади, аммо ташқи фаолликнинг юкланиши пасаяди. Натижада, шу тариқа ҳимояланувчи компьютер ички сервисларининг заифлиги пасаяди, чунки четки нияти бузуқ одам олдин, ҳимоялаш воситалари синчиклаб ва қатъий конфигурацияланган, экранни босиб ўтиши лозим.

Тақсимланган тармоқлараро экраннинг шахсий экрандан асосий фарқи-тақсимланган тармоқлараро экранда марказдан бошқариш функциясининг борлиги. Агар шахсий тармоқли экранлар улар ўрнатилган компьютер орқали бошқарилса (уй шароитида қўлланишга жуда мос), тақсимланган тармоқлараро экранлар ташкилотнинг бош офисида ўрнатилган бошқаришнинг умумий консоли томонидан бошқарилиши мумкин.

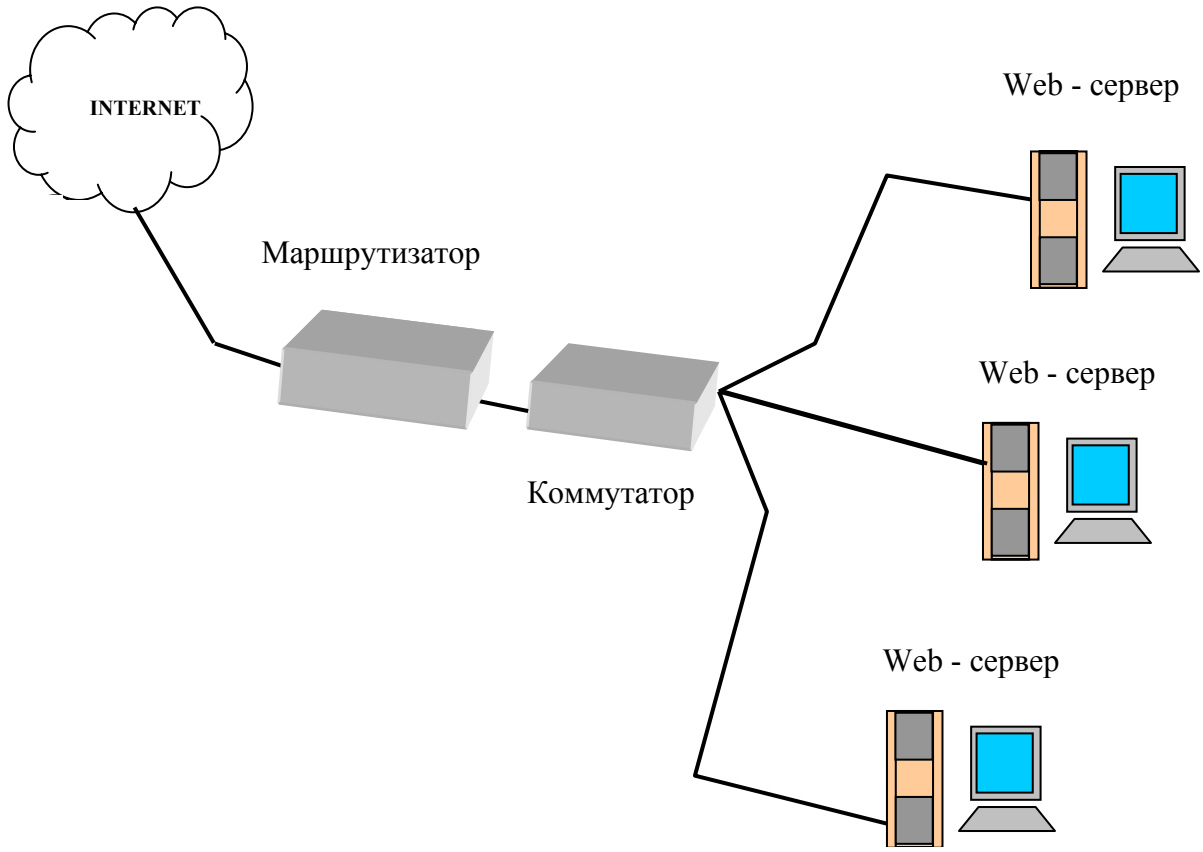
Корпоратив тармоқ рухсатсиз фойдаланишдан ҳақиқатан ҳам ҳимояланган ҳисобланади, қачонки унинг Internetдан кириш нуқтасида ҳимоя воситалари ҳамда ташкилот локал тармоғи фрагментларини, корпоратив серверларини ва алоҳида компьютерлар хавфсизлигини таъминловчи ечимлар мавжуд бўлса. Тақсимланган ёки шахсий тармоқлараро экран асосидаги ечимлар алоҳида компьютерлар, корпоратив серверлар ва ташкилот локал тармоқ фрагментлари хавфсизлигини таъминлашни аъло даражада бажаради.

Тақсимланган тармоқлараро экранлар, анъанавий тармоқлараро экранлардан фарқли равишда, қўшимча дастурий таъминот бўлиб, хусусан корпоратив серверларни, масалан Internet-серверларни ишончли ҳимоялаши

мумкин. Корпоратив тармоқни ҳимоялашнинг оқилона ечими – ҳимоялаш воситасини у ҳимоя қилувчи сервери билан бир платформада жойлаштиришдир. 7.16-расмда корпоратив серверларни тақсимланган тармоқлараро экранлар ёрдамида ҳимоялаш схемаси келтирилган.

Анъанавий ва тақсимланган тармоқлараро экранларни қуйидаги кўрсаткичлари бўйича таққослайлик.

Самарадорлик. Анъанавий брандмауэр кўпинча тармоқ периметрии бўйича жойлаштирилади, яъни у ҳимоянинг бир қатламини таъминлайди холос. Агар бу ягона қатлам бузилса, тизим ҳарқандай хужумга бардош бераолмайди. Шахсий брандмауэр операцион тизимнинг ядро сатҳида ишлайди ва барча кирувчи ва чиқувчи пакетларни текшириб корпоратив серверларни ишончли ҳимоялайди.



7.16 -расм. Тақсимланган тармоқлараро экранлар ёрдамида корпоратив серверларни ҳимоялаш

Ўрнатилишининг осонлиги. Анъанавий брандмауэр корпоратив тармоқ конфигурациясининг бўлими сифатида ўрнатилиши лозим. Тақсимланган брандмауэр дастурий таъминот бўлиб, саноқли дақиқаларда ўрнатилади ва олиб ташланади.

Бошқариш. Анъанавий брандмауэр тармоқ маъмури томонидан бошқарилади. Тақсимланган брандмауэр тармоқ маъмури ёки локал тармоқ фойдаланувчиси томонидан бошқарилиши мумкин.

Унумдорлик. Анъанавий брандмауэр тармоқлараро алмашишни таъминловчи қурилма бўлиб, унумдороиги (пакет/дақиқа бўйича) белгиланган чегараланишга эга. У бир-бири билан коммутацияланувчи маҳаллий тармоқ орқали боғланган ўсувчи сервер парклари учун тўғри келмайди. Тақсимланган брандмауэр қабул қилинган хавфсизлик сиёсатига зиён етказмасдан сервер паркларини ўсишига имкон беради.

Нархи. Анъанавий брандмауэр, одатда функциялари белгиланган, нархи етарлича юқори тизим ҳисобланади. Брандмауэрнинг тақсимланган маҳсулотлари дастурий таъминот бўлиб, анъанавий тармоқлараро экранлар нархининг 1/5 ёки 1/10 га тенг.

VIII боб. ҲИМОЯЛАНГАН ВИРТУАЛ ХУСУСИЙ ТАРМОҚЛАР

8.1. Ҳимояланган виртуал хусусий тармоқларни қуриш концепцияси

Internet нинг гуриллаб ривожланиши натижасида дунёда ахборотни тарқатиш ва фойдаланишда сифатий ўзгариш содир бўлди. Internet фойдаланувчилари арзон ва қулай коммуникацияга эга бўлдилар. Корхоналар Internet каналларидан жиддий тижорат ва бошқарув ахборотларини узатиш имкониятларига қизиқиб қолдилар. Аммо Internetнинг қурилиши принципи нияти бузуқ одамларга ахборотни ўғирлаш ёки атайин бузиш имкониятини яратди. Одатда TCP/IP протоколлар ва стандарт Internet-иловалар (e-mail, Web, FTP) асосида қурилган корпоратив ва идора тармоқлари суқилиб киришдан кафолатланмаганлар.

Internetнинг ҳамма ерда тарқалишидан манфаат кўриш мақсадида тармоқ хужумларига самарали қаршилик кўрсатувчи ва бизнесда очиқ тармоқлардан фаол ва хавфсиз фойдаланишга имкон берувчи виртуал хусусий тармоқ VPN яратиш устида ишлар олиб борилди. Натижада 1990 йилнинг бошида виртуал хусусий тармоқ VPN концепцияси яратилди. "Виртуал" ибораси VPN атамасига иккита узел ўртасидаги уланишни вақтинча деб кўрилишини таъкидлаш мақсадида киритилган. Ҳақиқатан, бу уланиш доимий, қатъий бўлмай, фақат очиқ тармоқ бўйича трафик ўтганида мавжуд бўлади.

Виртуал тармоқ VPNларни қуриш концепцияси асосида етарлича оддий ғоя ётади: агал глобал тармоқда ахборот алмашинувчи иккита узел бўлса, бу узеллар орасида очиқ тармоқ орқали узатилаётган ахборотнинг конфиденциаллигини ва яхлитлигини таъминловчи виртуал ҳимояланган туннел қуриш зарур ва бу виртуал туннелдан барча мумкин бўлган ташқи фаол ва пассив кузатувчиларнинг фойдаланиши хаддан ташқари қийин бўлиши лозим.

Шундай қилиб, VPN туннели очиқ тармоқ орқали ўтказилган уланиш бўлиб, у орқали виртуал тармоқнинг криптографик ҳимояланган ахборот

пакетлари узатилади. Ахборотни VPN туннели бўйича узатилиши жараёнидаги ҳимоялаш қуйидаги вазифаларни бажаришга асосланган:

- ўзаро алоқадаги тарафларни аутентификациялаш;
- узатилувчи маълумотларни криптографик беркитиш (шифрлаш);
- етказиладиган ахборотнинг ҳақиқийлигини ва яхлитлигини текшириш.

Бу вазифалар бир бирига боғлиқ бўлиб, уларни амалга оширишда ахборотни криптографик ҳимоялаш усулларидан фойдаланилади. Бундай ҳимоялашнинг самарадорлиги симметрик ва асимметрик криптографик тизимларнинг биргаликда ишлатилиши эвазига таъминланади. VPN қурилмалари томонидан шакллантирилувчи VPN туннели ҳимояланган ажратилган линия хусусиятларига эга бўлиб, бу ҳимояланган ажратилган линиялар умумфойдаланувчи тармоқ, масалан Internet доирасида, сафланади. VPN қурилмалари виртуал хусусий тармоқларда VPN-мижоз, VPN-сервер ёки VPN хавфсизлиги шлюзи вазифасини ўташи мумкин.

VPN-мижоз одатда шахсий компьютер асосидаги дастурий ёки дастурий-аппарат комплекси бўлиб, унинг тармоқ дастурий таъминоти у бошқа VPN-мижоз, VPN-сервер ёки VPN хавфсизлиги шлюзлари билан алмашинадиган трафикни шифрлаш ва аутентификациялаш учун модификацияланади. Одатда VPN-мижознинг амалга оширилиши стандарт операцион тизим – Windows NT/2000 ёки Unixни тўлдирувчи дастурий ечимдан иборат бўлади.

VPN-сервер сервер вазифасини ўтовчи, компьютерга ўрнатилувчи дастурий ёки дастурий-аппарат комплексидан иборат. VPN-сервер ташқи тармоқларнинг рухсатсиз фойдаланишидан серверларни ҳимоялашни ҳамда алоҳида компьютерлар ва мос VPN-маҳсулотлари орқали ҳимояланган локал тармоқ сегментларидаги компьютерлар билан ҳимояланган уланишларни ташкил этишни таъминлайди. VPN-сервер VPN-мижознинг сервер платформалари учун функционал аналог ҳисобланади. У аввало VPN-мижозлар билан кўпгина уланишларни мададловчи кенгайтирилган ресурслари билан ажралиб туради. VPN-сервер мобил фойдаланувчилар билан уланишларни ҳам мададлаши мумкин.

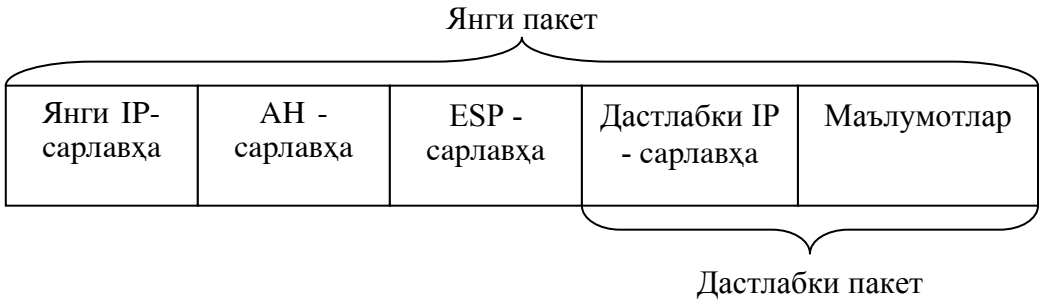
VPN хавфсизлик шлюзи. (Security gateway) иккита тармоққа уланувчи тармоқ қурилмаси бўлиб, ўзидан кейин жойлашган кўп сонли хостлар учун шифрлаш ва аутентификациялаш вазифаларини бажаради. VPN хавфсизлиги шлюзи шундай жойлаштириладики, ички корпоратив тармоққа аталган барча трафик у орқали ўтади. VPN хавфсизлиги шлюзининг адреси кирувчи туннелланувчи пакетнинг ташқи адреси сифатида кўрсатилади, пакетнинг ички адреси эса шлюз орқасидаги муайян хост адреси ҳисобланади. VPN хавфсизлиги шлюзи алоҳида дастурий ечим, алоҳида аппарат қурилмаси, ҳамда VPN вазифалари билан тўлдирилган маршрутизаторлар ёки тармоқлараро экран кўринишида амалга оширилиши мумкин.

Ахборот узатишнинг очиқ ташқи муҳити маълумот узатишнинг тезкор каналларини (Internet муҳити) ва алоқанинг секин ишлайдиган умумфойдаланувчи каналларини (масалан, телефон тармоғи каналларини) ўз ичига олади. Виртуал хусусий тармоқ VPNнинг самарадорлиги алоқанинг очиқ каналлари бўйича айланувчи ахборотнинг ҳимояланиш даражасига боғлиқ. Очиқ тармоқ орқали маълумотларни хавфсиз узатиш учун инкапсуляциялаш ва туннеллаш кенг ишлатилади. Туннеллаш усули бўйича маълумотлар пакети умумфойдаланувчи тармоқ орқали худди оддий икки нуқтали уланиш бўйича узатилганидек узатилади. Ҳар бир "жўнатувчи-қабул қилувчи" жуфтлиги орасига бир протокол маълумотларини бошқасининг пакетига инкапсуляциялашга имкон берувчи ўзига хос туннел-мантиқий уланиш ўрнатилади.

Туннеллашга биноан, узатилувчи маълумотлар порцияси хизматчи ҳошиялар билан бирга янги "конверт"га "жойлаш" амалга оширилади. Бунда пастроқ сатҳ протоколи пакети юқорироқ ёки худи шундай сатҳ протоколи пакети маълумотлари майдонига жойлаштирилади. Таъкидлаш лозимки, туннелашнинг ўзи маълумотларни рухсатсиз фойдаланишдан ёки бузишдан ҳимояламайди, аммо туннеллаш туфайли инкапсуляцияланувчи дастлабки пакетларни тўла криптографик ҳимоялаш имконияти пайдо бўлади. Узатилувчи маълумотлар конфиденциаллигини таъминлаш мақсадида жўнатувчи дастлабки пакетларни шифрлайди, уларни, янги IP-

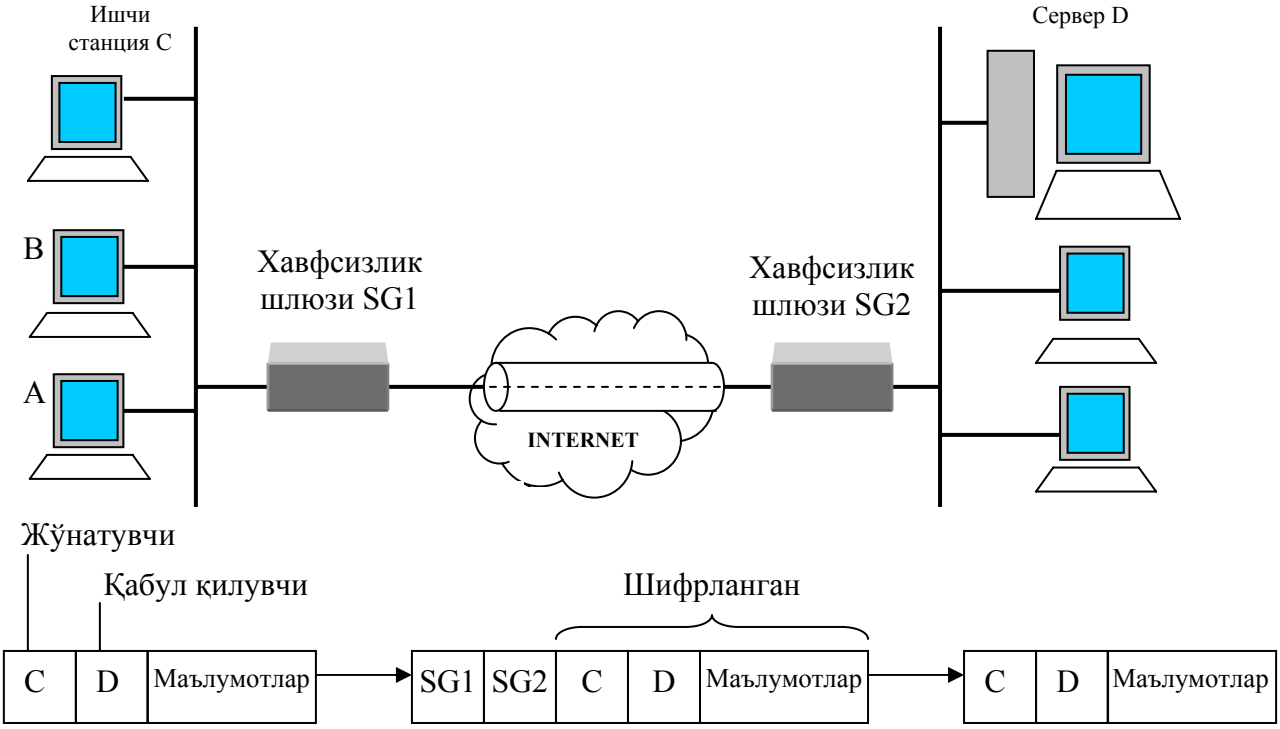
сарлавҳа билан ташқи пакетга жойлайди ва транзит тармоқ бўйича жўнатади (8.1-расм).

Очиқ тармоқ бўйича маълумотларни ташишда ташқи пакет сарлавҳасининг очиқ каналларидан фойдаланилади.



8.1-расм. Туннеллашга тайёрланган пакет мисоли

Ташқи пакет ҳимояланган каналнинг охирги нуқтасига келиши билан ундан ички дастлабки пакет чиқариб олиниб, расшифровка қилинади ва унинг тикланган сарлавҳаси ички тармоқ бўйича кейинги узатиш учун ишлатилади (8.2-расм)



8.2-расм. Виртуаль ҳимояланган туннел схемаси.

Туннеллашдан пакет таркибини нафақат конфиденциаллигини, балки унинг яхлитлигини ва аутентилигини таъминлашда фойдаланилади. Бунда электрон рақамли имзони пакетнинг барча ҳошияларига тарқатиш мумкин.

Internet билан боғланмаган локал тармоқ яратилганда компания ўзининг тармоқ қурилмалари ва компьютерлари учун ҳоҳлаган IP-адресдан фойдаланиши мумкин. Олдин яккаланган тармоқларни бирлаштиришда бу адреслар бир-бирлари ва Internetда ишлатилаётган адреслар билан тўқнашишлари мумкин. Пакетларни инкапсуляциялаш бу муаммони ечади, чунки у дастлабки адресларни беркитишга ва Internet IP адреслари маконидаги ноёб адресларни қўшишга имкон беради. Бу адреслар кейин маълумотларни ажратилувчи тармоқлар бўйича узатишда ишлатилади. Бунга локал тармоққа уланувчи мобил фойдаланувчиларнинг IP-адресларини ва бошқа параметрларини созлаш масаласи ҳам киради.

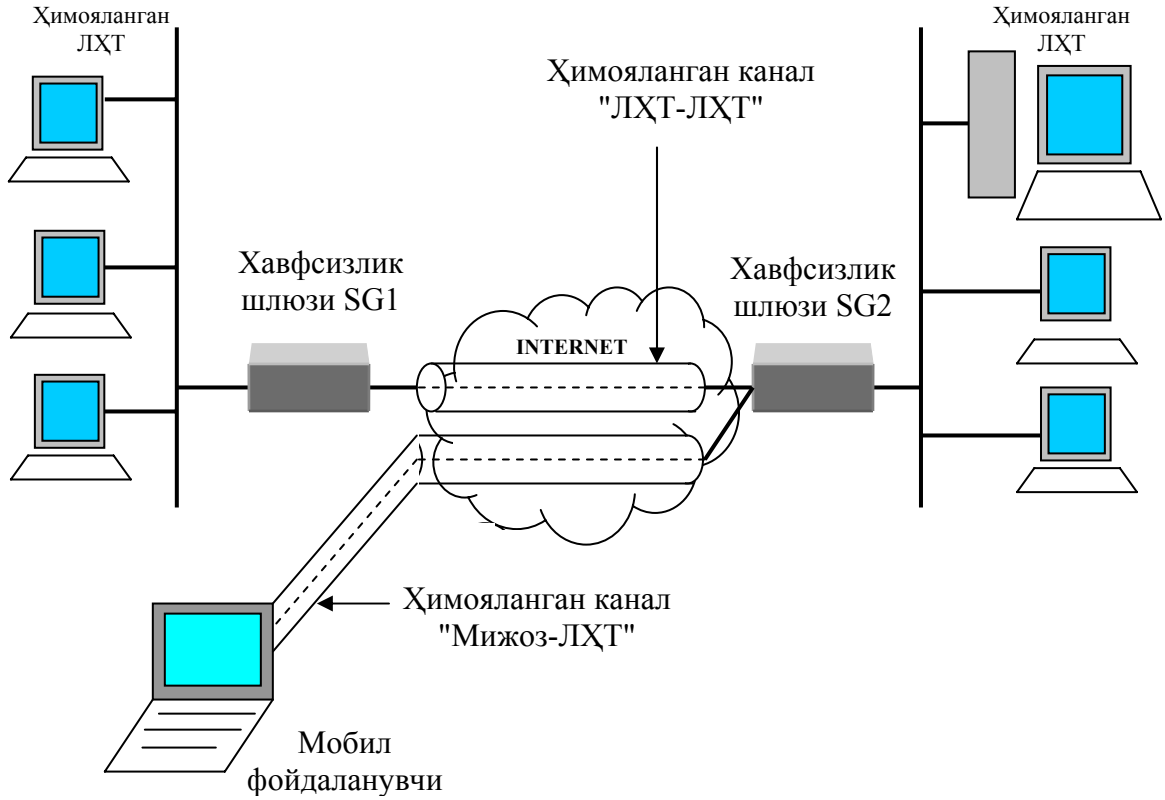
Тунеллаш механизми ҳимояланувчи канални шакллантирувчи турли протоколларда кенг қўлланилади. Одатда туннел фақат маълумотларнинг конфиденциаллиги ва яхлитлигининг бузилиши хавфи мавжуд бўлган очиқ тармоқ қисмида, масалан, очиқ Internet ва корпоратив тармоқ кириш нуқталари орасида, яратилади. Бунда ташқи пакетлар учун ушбу икки нуқтада ўрнатилган чегара маршрутизаторларининг адресларидан фойдаланилса, охирги узелларнинг ички адреслари ички дастлабки пакетларда ҳимояланган ҳолда сақланади. Таъкидлаш лозимки, тунеллаш механизмининг ўзи қандай мақсадларда туннеллаш қўлланилаётганига боғлиқ эмас. Туннеллаш нафақат узатилаётган барча маълумотларнинг конфиденциаллиги ва яхлитлигини таъминлашда, балки турли протоколли (масалан IPv4 ва IPv6) тармоқлар орасида ўтишни ташкил этишда ҳам қўлланилади. Туннеллаш бир протокол пакетини бошқа протоколдан фойдаланувчи мантиқий муҳитда узатишни ташкил этишга имкон беради. Натижада бир неча турли хил тармоқларнинг ўзаро алоқалари муаммосини ҳал этиш имконияти пайдо бўлади.

Туннеллаш механизмини амалга оширилишига уч хил протоколлар: протокол-"йўловчи", протокол элтувчи ва туннеллаш протоколи ишлаши натижаси деб қараш мумкин. Масалан, протокол - "йўловчи" сифатида битта корхона филиалларининг локал тармоқларида маълумотларни ташувчи транспорт протоколи IPX ишлатилиши мумкин. Элтувчи протоколнинг энг кўп тарқалган варианти Internet тармоғининг IP протоколи

ҳисобланади. Туннеллаш протоколи сифатида канал сатҳи протоколари PPTP ва L2TP, ҳамда тармоқ сатҳи протоколи IPSec ишлатилиши мумкин. Туннеллаш туфайли Internet инфратузилмасини VPN-иловалардан беркитиш мумкин бўлади.

VPN туннеллари турли фойдаланувчилар учун яратилиши мумкин. булар хавфсизлик шлюзи бўлган *локал тармоқ* LAN ёки масофадаги ва мобил фойдаланувчиларнинг алоҳида компьютерлари бўлиши мумкин. Йирик корхонанинг виртуал хусусий тармоғини яратиш учун VPN-шлюзлар, VPN-серверлар ва VPN-мижозлар керак бўлади. VPN-шлюзларни корхона локал тармоқларини ҳимоялаш учун ишлатиш мақсадга мувофиқ бўлса, VPN-серверлар ва VPN-мижозлардан масофадаги ва мобил фойдаланувчиларни Internet орқали корпоратив тармоқ билан ҳимояланган уланишини ташкил этишда фойдаланилади.

Виртуал ҳимояланган каналларни қуриш вариантлари. VPN ни лойиҳалашда одатда иккита асосий схема кўрилади (8.3-расм):



8.3-расм. "ЛҲТ-ЛҲТ" ва "Мижоз-ЛҲТ" хилидаги виртуал ҳимояланган каналлар

- локал тармоқлар орасидаги виртуал ҳимояланган канал ("ЛХТ-ЛҲТ" канал);

- узел ва локал тармоқ орасидаги виртуал ҳимояланган канал ("мижоз-ЛҲТ" канали).

Уланишнинг биринчи схемаси алоҳида офислар орасидаги қимматли ажратилган линиялар ўрнига ўтади ва улар орасида доимо фойдаланувчан, ҳимояланган каналларни яратади. Бу ҳолда хавфсизлик шлюзи туннел ва локал тармоқ орасида интерфейс вазифасини ўтайди ва локал тармоқ фойдаланувчилари бир-бирлари билан мулоқот қилишда туннелдан фойдаланадилар. Аксарият компаниялар VPNнинг бу ҳилидан глобал тармоқнинг мавжуд Frame Relay каби уланишларни алмаштириш учун ёки уларга қўшимча сифатида фойдаланадилар.

VPN ҳимояланган каналнинг иккинчи схемаси масофадаги ёки мобил фойдаланувчилар билан уланишни ўрнатишга аталган. Туннелни яратишни мижоз (масофадан фойдаланувчи) бошлаб беради. Масофадаги тармоқни ҳимояловчи шлюз билан боғланиш учун у ўзининг компьютерида махсус мижоз дастурий таъминотини ишга туширади. VPNнинг бу тури коммутацияланувчи уланишларни ўрнига ўтади ва масофадан фойдаланишнинг анъанавий усуллари билан бир қаторда ишлатилиши мумкин.

Виртуал ҳимояланган каналларнинг қатор вариантлари мавжуд. Умуман, орасида виртуал ҳимояланган канал шакллантирилувчи корпоратив тармоқнинг ҳар қандай иккита узели ҳимояланувчи ахборот оқимининг охирги ва оралиқ нуқтасига тааллуқли бўлиши мумкин. Ахборот хавфсизлиги нуқтаи назаридан ҳимояланган туннел охирги нуқталарининг ҳимояланувчи ахборот оқимининг охирги нуқталарига мос келиши варианти маъқул ҳисобланади. Бу ҳолда каналнинг ахборот пакетлари ўтишининг барча йўллари бўйлаб ҳимояланиши таъминланади. Аммо бу вариант бошқаришнинг децентрализацияланишига ва ресурс сарфининг ошишига олиб келади. Агар виртуал тармоқдаги локал тармоқ ичида трафикни ҳимоялаш талаб этилмаса, ҳимояланган туннелнинг охирги нуқтаси сифатида ушбу локал тармоқнинг тармоқлараро экрани ёки чегара маршрутизатори танланиши мумкин. Агар локал тармоқ ичидаги ахборот оқими

ҳимояланиши шарт бўлса, бу тармоқ охирги нуқтаси вазифасини ҳимояланган алоқада иштирок этувчи компьютер бажаради.

Локал тармоқдан масофадан фойдаланилганида фойдаланувчи компьютери виртуал ҳимояланган каналнинг охирги нуқтаси бўлиши шарт. Фақат пакетларни коммутациялашли очиқ тармоқ, масалан Internet ичида ўтказилувчи ҳимояланган туннел варианти етарлича кенг тарқалган. Ушбу вариант ишлатилиши қулайлиги билан ажралиб турсада, нисбатан паст хавфсизликка эга. Бундай туннелнинг охирги нуқталари вазифасини одатда Internet провайдерлари ёки локал тармоқ чегара маршрутизаторлари (тармоқлараро экранлар) бажаради.

Локал тармоқлар бирлаштирилганида туннел фақат Internetнинг чегара провайдерлари ёки локал тармоқнинг маршрутизаторлари (тармоқлараро экранлари) орасида шакллантирилади. Локал тармоқдан масофадан фойдаланилганида туннел Internet провайдерининг масофадан фойдаланиш сервери, ҳамда Internetнинг чегара провайдери ёки локал тармоқ маршрутизатори (тармоқлараро экран) орасида яратилади. Ушбу вариант бўйича қурилган корпоратив тармоқлар яхши масштабланувчанлик ва бошқарилувчанликка эга бўлади. Шакллантирилган ҳимояланган туннеллар ушбу виртуал тармоқдаги мижоз компьютерлари ва серверлари учун тўла шаффоф ҳисобланади. Ушбу узелларнинг дастурий таъминоти ўзгармайди. Аммо бу вариант ахборот алоқасининг нисбатан паст хавфсизлиги билан характерланади, чунки трафик қисман очиқ алоқа канали бўйича ҳимояланмаган ҳолда ўтади. Агар шундай VPNни яратиш ва эксплуатация қилишни провайдер ISP ўз зиммасига олса, барча виртуал хусусий тармоқ унинг шлюзларида, локал тармоқлар ва корхоналарнинг масофадаги фойдаланувчилари учун шаффоф ҳолда қурилиши мумкин. Аммо бу ҳолда провайдерга ишонч ва унинг хизматига доимо тўлаш муаммоси пайдо бўлди.

Ҳимояланган туннел, орасида туннел шакллантирилувчи узеллардаги виртуал тармоқ компонентлари ёрдамида яратилади. Бу компонентларни туннел инициаторлари ва туннел терминаторлари деб юритиш қабул қилинган.

Туннел инициатори дастлабки пакетни янги пакетга жўнатувчи ва қабул қилувчи хусусидаги ахбороти бўлган янги сарлавҳали пакетга инкапсуляциялайди. Инкапсуляцияланган пакетлар ҳар қандай протокол турига, жумладан маршрутланмайдиган протоколларга (масалан Net BEUL) мансуб бўлишлари мумкин. Туннел бўйича узатиладиган барча пакетлар IP пакетлари ҳисобланади. Туннелнинг инициатори ва терминатори орасидаги маршрутни одатда, Internetдан фарқланиши мумкин бўлган, оддий маршрутланувчи тармоқ IP аниқлайди.

Туннелни инициаллаш ва узиш турли тармоқ қурилмалари ва дастурий таъминот ёрдамида амалга оширилиши мумкин. Масалан, туннел масофадан фойдаланиш учун улашни таъминловчи модем ва мос дастурий таъминот билан жиҳозланган мобил фойдаланувчининг ноутбуки томонидан инициалланиши мумкин. Инициатор вазифасини мос функционал имкониятларга эга бўлган локал тармоқ маршрутизатори ҳам бажариши мумкин. Туннел одатда, тармоқ коммутатори ёки хизматлар провайдери шлюзи билан тугалланади.

Туннел терминатори инкасуляциялаш жараёнига тескари жараённи бажаради. Терминатор янги янги сарлавҳаларни олиб ташлаб, ҳар бир дастлабки пакетни локал тармоқдаги адресатга йўллайди.

Инкапсулацияланувчи пакетларнинг конфиденциаллиги уларни шифрлаш, яхлитлиги ва ҳақиқийлиги эса электрон рақамли имзони шакллантириш йўли билан таъминланади. Маълумотларни криптографик ҳимоялашнинг жўда кўп усуллари ва алгоритмлари мавжуд бўлганлиги сабабли, туннел инициатори ва терминатори ҳимоянинг бир хил усулларидан фойдаланишга ўз вақтида келишиб олишлари мақсадга мувофиқ ҳисобланади. Маълумотларни расшифровка қилиш ва рақамли имзони текшириш имкониятини таъминлаш учун туннел инициатор ива терминатори калитларни хавфсиз алмашиш вазифасини ҳам мададлашлари зарур. Ундан ташқари, VPN туннеларини ваколатли фойдаланувчилар томонидан яратилишини кафолатлаш мақсадида ахборот алоқасининг асосий тарафлари аутентификациялашдан ўтишлари лозим. Корпорациянинг мавжуд

тармоқ инфратузилмалари VPNдан фойдаланишга ҳам дастурий, ҳам аппарат таъминот ёрдамида тайёрланишлари мумкин.

8.2. Ҳимояланган виртуал хусусий тармоқларнинг туркумланиши

Ҳимояланган виртуал хусусий тармоқлар VPNни туркумлашни турли вариантлари мавжуд. Кўпинча туркумлашнинг қуйидаги учта аломати ишлатилади:

- OSI моделининг иш сатҳи;
- VPN техник ечимининг архитектураси;
- VPNни техник амалга ошириш усули.

OSI моделининг иш сатҳи бўйича VPNнинг туркумланиши. Ушбу туркумлаш анчагина қизиқиш тўғдиради, чунки амалга оширилувчи VPNнинг функционаллиги ва унинг корпоратив ахборот тизимлари иловалари ҳамда ҳимоянинг бошқа воситалари билан биргаликда ишлатилиши кўп ҳолларда танланган OSI сатҳига боғлиқ бўлади.

OSI моделининг иш сатҳ аломати бўйича канал сатҳидаги VPN, тармоқ сатҳидаги VPN ва сеанс сатҳидаги VPN фарқланади. Демак, VPNлар одатда OSI моделининг пастки сатҳларида қурилади. Бунинг сабаби шуки, ҳимояланган канал воситалари қанчалик пастки сатҳда амалга оширилса, уларни иловаларга ва татбиқий протоколларга шунчалик шаффоф қилиш соддалашади. Тармоқ ва канал сатҳларида иловаларнинг ҳимоя протоколларига боғлиқлиги умуман йўқолади. Шу сабабли, фойдаланувчилар учун универсал ва шаффоф ҳимояни фақат OSI моделининг пастки сатҳларида қуриш мумкин. Аммо, бунда биз бошқа муаммога-ҳимоя протоколининг муайян тармоқ технологиясига боғлиқлиги муаммосига дуч келамиз.

Каналь сатҳидаги VPN. OSI моделининг канал сатҳида ишлатилувчи VPN воситалари учинчи (ва юқорироқ) сатҳнинг турли хил трафигини инкапсулациялашни таъминлашга ва "нуқта-нуқта" тилидаги виртуал туннелларни (маршрутизатордан маршрутизаторга ёки шахсий компьтердан локал ҳисоблаш тармоғининг шлюзигача) қуришга имкон беради. Бу гуруҳга L2F

(Layer 2 Forwarding) ва PPTP (Point-to-Point Tunneling Protocol) протоколлари ҳамда Cisco Systems и MicroSoft фирмаларининг бирга ишлаб чиққан L2TP(Layer 2 Tunneling Protocol) стандартидан фойдаланувчи VPN-маҳсулотлар тааллуқли.

Ҳимояланган каналнинг протоколи PPTP "нуқта-нуқта" уланишларида, масалан, ажратилган линияларда ишлаганда кенг қўлланилувчи PPP протоколига асосланган. PPTP протоколи иловалари ва татбиқий сатҳ хизматлари учун ҳимоя воситаларининг шаффофлигини таъминлайди ва тармоқ сатҳида ишлатилувчи протоколга боғлиқ эмас. Хусусан, PPTP протоколи ҳам IP тармоқларида, ҳам IPX, DECnet ёки NetBEUL протоколлари асосида ишловчи тармоқларда пакетларни ташиши мумкин. Аммо, PPP протоколи ҳамма тармоқларда ҳам ишлатилмаслиги сабабли (аксарият локал тармоқларида канал сатҳида Ethernet протоколи ишласа, глобал тармоқларда ATM, Frame Relay тармоқлари ишлайди), уни универсал восита деб беўлмайди. Йирик бирикма тармоқнинг турли қисмларида, умуман айтганда, турли канал протоколлари ишлатилади. Шу сабабли бу гетероген муҳит орқали канал сатҳининг ягона протоколи ёрдамида ҳимояланган каналнни ўтказиш мумкин эмас.

L2TP протоколи, эҳтимол, локал ҳисоблаш тармоқларидан фойдаланишни ташкил этишда устунлик қилувчи ечим бўлиб қолиши мумкин (чунки у, асосан, Windows операцион тизимига таянади.)

Тармоқ сатҳидаги VPN. Тармоқ сатҳидаги VPN-маҳсулотлар IPни IPга инкапсуляциялашни бажаради. Бу сатҳдаги кенг тарқалган протоколлардан бири SKIP протоколидир. Аммо бу протоколни аутентификациялаш, туннеллаш ва IP-пакетларни шифрлаш учун аталган IPSec(IPSecurity) протоколи аста-секин суриб чиқармоқда.

Тармоқ сатҳида ишловчи IPSec протоколи муросага асосланган вариант ҳисобланади. Бир томондан у иловадар учун шаффоф, иккинчи томондан кенг тарқалган IP протоколига асосланганлиги сабабли барча тармоқларда ишлаши мумкин. Шу орада эсдан чиқармаслик лозимки, IPSecнинг спецификацияси IPга мўлжалланганлиги сабабли у тармоқ сатҳининг бошқа протоколлари трафиги учун тўғри келмайди. IPSec прото-

коли L2TP протоколи билан биргаликда ишлаши мумкин. Натижада бу икки протокол ишончли идентификациялашни, стандартланган шифрлашни ва маълумотлар яхлитлигини таъминлайди. Иккита локал тармоқ орасидаги IPSecтуннели маълумотлар узатувчи якка тармоқлар тўпламини мададлаши мумкин. Натижада бу хилдаги иловалар масштабланиш нуқтаи назаридан иккинчи сатҳ технологияларига нисбатан устунликка эга бўлади.

IPSec протоколи билан масофадаги қурилмалар орасида криптографик калитларни хавфсиз бошқариш ва алмашиш масалаларини ечувчи IKE (Internet Key Exchange) протоколи боғланган. IKE протоколи калитларни алмашишни автоматлаштиради ва химояланган уланишни ўранатади, IPSec эса пакетларни кодлайди ва "имзо чекади". Ундан ташқари, IKE ўрнатилган уланиш учун калитни ўзгартириш имкониятига эга. Бу узатилувчи ахборотнинг конфиденциаллигини оширади.

Сеанс сатҳидаги VPN. Баъзи VPNлар "канал воситачилари" (circuit proxy) деб аталувчи усулдан фойдаланади. Бу усул транспорт сатҳи устида ишлайди ва ҳар бир сокет учун алоҳида трафикни ҳимояланган тармоқдан умумфойданувчи Internet тармоғига ретрансляциялайди. (IP сокети TCP-уланишнинг ва муайян порт ёки берилган порт UDP комбинацияси орқали идентификацияланади. TCP/IP стекида бешинчи-сеанс сатҳи бўлмайди, аммо сокетларга мўлжалланган амалларни кўпинча сеанс сатҳи амаллари деб юритишади.)

Туннелнинг инициатори ва терминатори орасида узатилувчи ахборотни шифрлаш транспорт сатҳи TLS(Transport Layer Security) ёрдамида амалга оширилади. Тармоқлараро экран орқали аутентификацияланган ўтишни стандартлаш учун SOCKS деб аталувчи протокол аниқланган ва ҳозирда SOCKS протоколининг 5-версияси канал воситачиларини стандарт амалга оширилишида ишлатилади.

SOCKS протоколининг 5-версиясида мижоз компьютери воситачи (proxy) вазифаларини бажарувчи сервер билан аутентифкацияланган сокет (ёки сеанс) ўрнатади. Бу воситачи-тармоқлараро экран орқали боғланишнинг ягона усули. Воситачи, ўз навбатида, мижоз томонидан сўралган ҳар қандай амални бажаради. Воситачига сокет сатҳидаги трафик

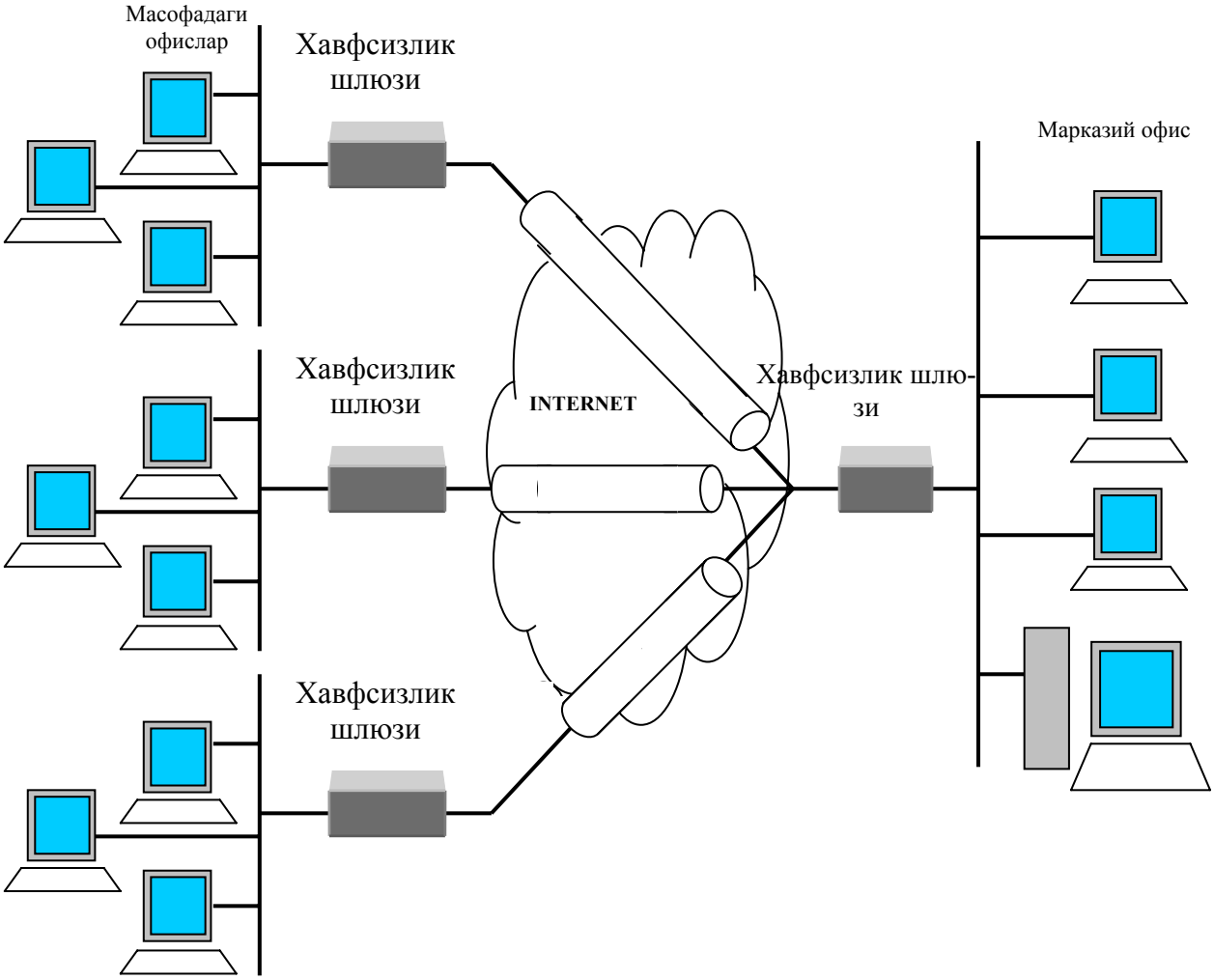
маълумлиги сабабли, у синчиклаб назорат қилиши, масалан, муайян иловаларни, агар улар зарурий ваколатларга эга бўлмаса, блокировка қилиши мумкин.

Агар IPSec протоколи моҳияти бўйича, IP тармоқни ҳимояланган туннелга тарқатса, SOCKS протоколи асосидаги маҳсулотлар уни алоҳида ҳар бир илова ва ҳар бир сокетга кенгайтиради. Иккинчи ва учинчи сатҳнинг яратилган туннеллари иккала йўналишда бирдай ишласа, 5 сатҳнинг VPN тармоғи ҳар бир йўналишда узатишни мустақил бошқаришга рухсат беради. IPSec протоколга ва иккинчи сатҳ протоколларига ўхшаб 5 сатҳнинг VPN тармоғини виртуал хусусий тармоқларнинг бошқа турлари билан бирга ишлатилиши мумкин, чунки бу технологиялар бир-бирини инкор қилмайди.

Техник ечимининг архитектураси бўйича VPNнинг туркумланиши. Ушбу туркумлаш бўйича виртуал хусусий тармоқлар қуйидаги уч турга бўлинади:

- корпорация ичидаги VPN тармоқ;
- масофадан фойдаланилувчи VPN тармоқ;
- корпорацияларо VPN тармоқ.

Корпорация ичидаги VPN тармоқ. Корпорация ичидаги VPN тармоқлар (Intranet VPN) корхона ичидаги бўлинмалар ёки алоқанинг корпорация тармоқлари (шу жумладан, ажратилган линиялар) ёрдамида бирлаштирилган корхоналар гуруҳи орасида ҳимояланган алоқани ташкил этиш учун ишлатилади. Ўзининг филиаллари ва бўлимлари учун ахборотнинг марказлаштирилган омборидан фойдаланишга эҳтиёж сезган компаниялар масофадаги узелларни ажратилган линиялар ёки frame relay технологияси ёрдамида улайдилар. Аммо ажратилган линияларнинг ишлатилиши эгалланадиган ўтказиш полосасининг ва объектлар орасидаги масофанинг катталашгани сари жорий сарф-ҳаражатларнинг ошишига сабаб бўлади. Буларни камайтириш учун компания узелларини виртуал хусусий тармоқ ёрдамида улаши мумкин (8.4-расм).



8.4-расм. VPN intranet технологияси ёрдамида тармоқ узелларини улаш.

Intranet VPN тармоқлар Internetдан ёки сервис-провайдерлар томонидан тақдим этилувчи бўлинувчи тармоқ инфратузилмаларидан фойдаланган ҳолда қурилади. Компания нархи қиммат ажратилган линиялардан воз кечиб, уларни арзонроқ Internet орқали алоқа билан алмаштиради. Бу ўтказиш полосасидан фойдаланишдаги сарф-ҳаражатни жиддий камайтиради, чунки Internetда масофа уланиш нархига ҳеч таъсир этмайди.

Intranet VPN учун қуйидаги афзалликлар характерли:

- конфиденциал ахборотни ҳимоялаш учун шифрлашнинг кучли криптографик протоколларидан фойдаланиш;

- автоматлаштирилган савдо тизими ва маълумотлар базасини бошқариш тизими каби жиддий иловаларни бажаришда ишлашининг ишончлилиги;

- сони тез ўсаётган фойдаланувчилар, янги офислар ва янги дастурий иловаларни самаралироқ жойлаштириш учун бошқаришнинг мослашувчанлиги.

Internetдан фойдаланиб Intranet VPNни қуриш VPN-технологияни амалга оширувчи энг рентабел усули ҳисобланади. Аммо Internetда сервис даражаси умуман кафолатланмайди. Кафолатланган сервис даражасини ҳоҳловчи компаниялар ўзларининг VPNларини сервер-провайдерлари томонидан тақдим этилувчи бўлинувчи тармоқ инфтузилмаларидан фойдаланиб сафлаш имкониятларини кўришлари шарт.

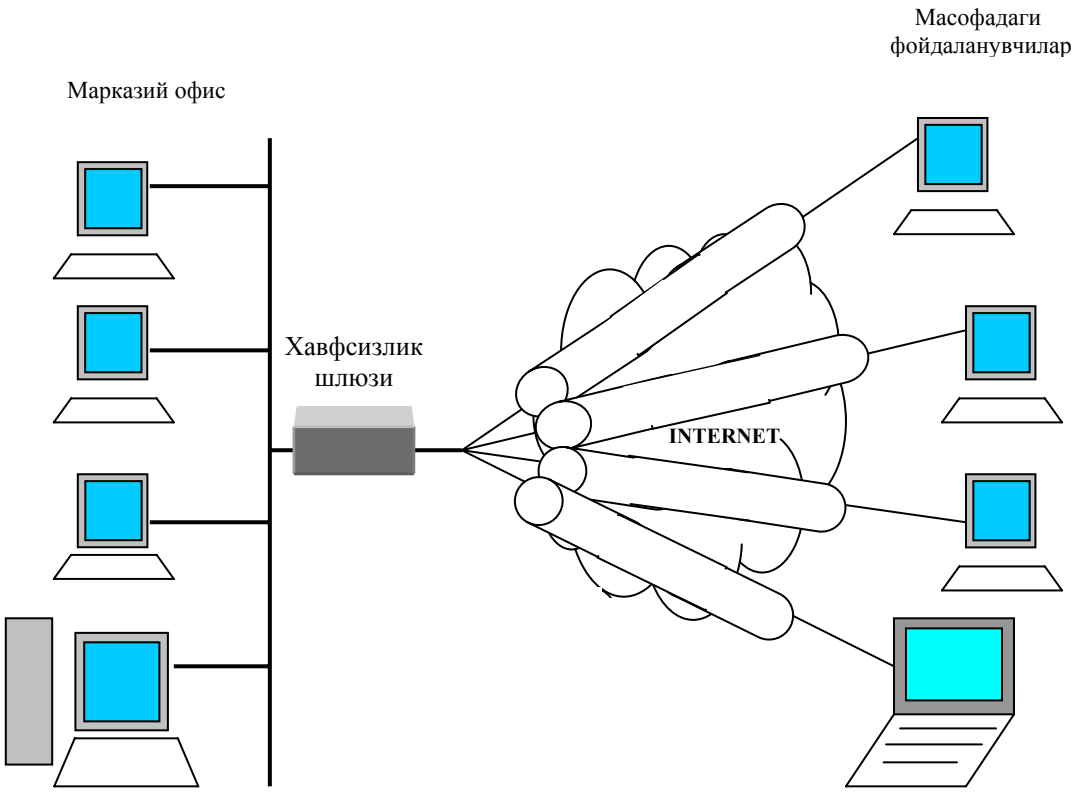
Масофадан фойдаланилувчи VPN тармоқ. Масофадан фойдаланилувчи виртуал хусусий тармоқлар VPN (Remote Access VPN) корпорациянинг мобил ёки масофадаги ходимларига (компания раҳбарияти, меҳнат сафаридаги ходимлар, касаначилар ва ҳ.) корхона ахборот ресурсларидан ҳимояланган масофадан фойдаланишни таъминлайди.

Масофадан фойдаланувчи виртуал хусусий тармоқларнинг (8.5-расм) коммутацияланувчи ва ажратилган линиялардан фойдаланишнинг ҳар ойдаги сарф-ҳаражатларини анчагина камайтиришга имкон бериши, уларнинг умумий эътироф этилишига сабаб бўлди. Уларнинг ишлаш принципи оддий: фойдаланувчилар глобал тармоқдан фойдаланишнинг маҳаллий нуқтаси билан уланишларни ўрнатади. Сўнгра уларнинг сўровлари Internet орқали туннелланади. Бу шаҳарлараро ва халқаро алоқа учун тўловдан қутилишга имкон беради. Ундан кейин барча сўровлар мос узелларда тўпланади ва корпорация тармоқларига узатилади.

Хусусий бошқарилувчи тармоқлардан (dial networks) масофадан фойдаланилувчи VPN тармоқларга (Remote Acces VPN) ўтиш қуйидаги афзалликларни беради:

- шаҳарлараро номерлар ўрнига маҳаллий номерлардан фойдаланиш имконияти шаҳарлараро телекоммуникацияга сарф-ҳаражатларни анчагина камайтиради;

- аутентификациялаш жараёнини ишончли ўтказишни таъминловчи масофадаги ва мобил фойдаланувчилар ҳақиқийлигини аниқлаш тизимининг самарадорлиги;



7.5-расм. Масофадан фойдаланишли виртуаль хусусий тармоқ.

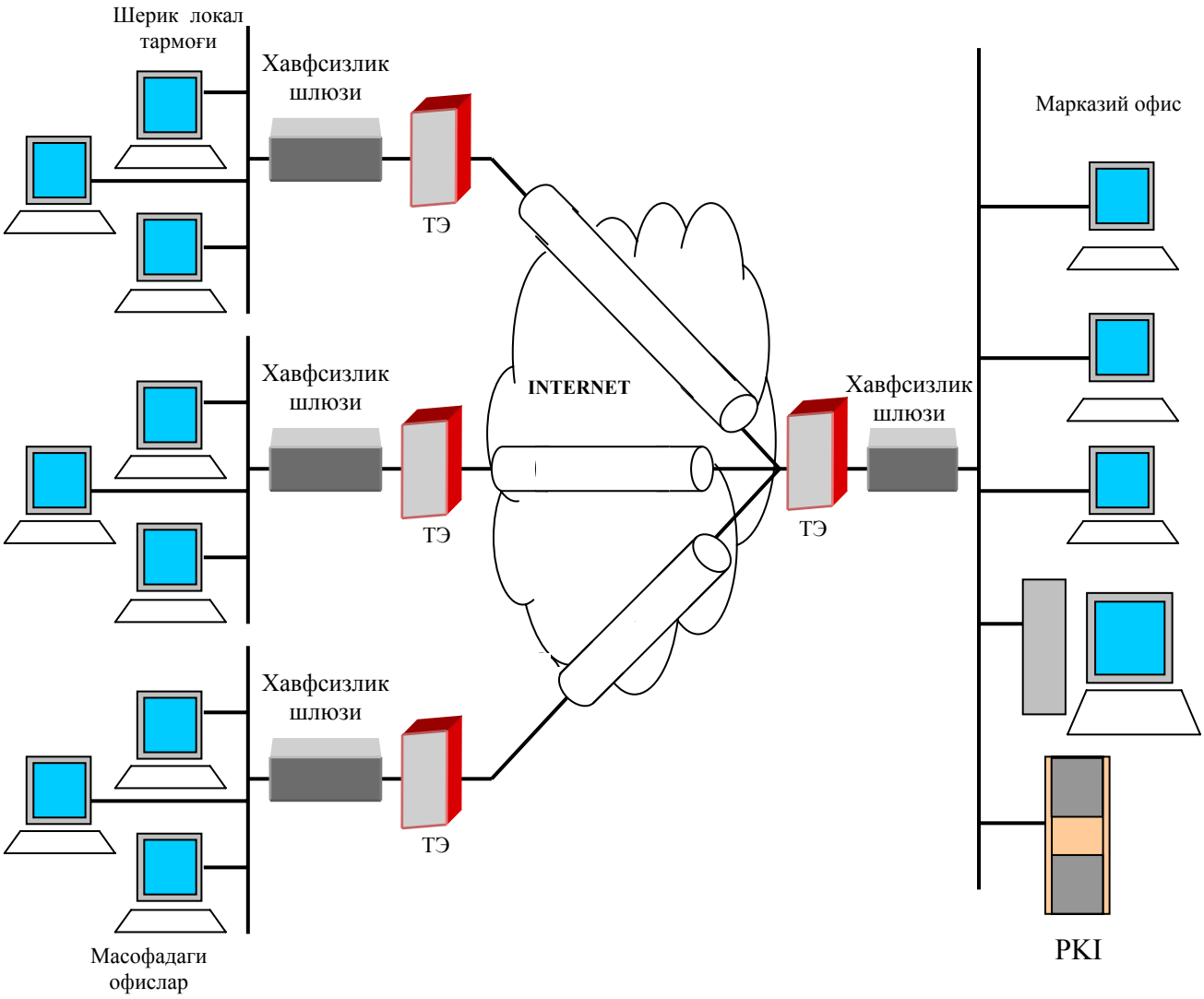
- масштабланишнинг янада юқорилиги ва тармоққа қўшилувчи янги фойдаланувчилар сафланишининг оддийлиги;

- компания эътиборини тармоқ ишлаши муаммолари ўрнига асосий корпорация бизнес-мақсадларига қаратиш.

Таъкидлаш лозимки, сезувчан корпорация трафигини ташишда очиқ тармоқ Internetнинг бирлаштирувчи магистрал сифатида ишлатилишининг масштаби ошиб бормоқда. Бу ахборот ҳимояси механизмини ушбу технологиянинг энг муҳим элементига айлантиради.

Корпорацияларараро VPN тармоқ. Корпорацияларараро VPN тармоқлардан (Extranet VPN) бизнес бўйича стратегик шериклар, хусусан чет эл асосий таъминотчилар, йирик буюртмачилар, мижозлар ва ҳ. билан самарали алоқани ва ахборотни ҳимояланган алмашинувини ташкил этишда фойдаланилади (8.6-расм).

Extranet – бир компания тармоғидан иккинчи компания тармоғининг тўғридан-тўғри фойдаланишини таъминлаш орқали иш юзасидан ҳамкорлик жараёнида алоқа ишончлилигини оширишга имкон берувчи технологиядир.



8.6-расм. Корпорацияларо extranet VPN тармоғи.

Extranet VPN тармоқлари умуман корпорация ичидаги виртуал хусусий тармоқларга ўхшаш, фарқи шундаки, корпорацияларо виртуал хусусий тармоқлар учун ахборот ҳимояси муаммоси кескинроқдир. Extranet VPN учун ишбилармон шериклар ўзларининг тармоқларида қўллашлари мумкин бўлган турли VPN-ечимлар билан алоқа қилиш имкониятларини кафолатловчи стандартлаштирилган VPN-маҳсулотлардан фойдаланиш характерлидир.

Бир неча компаниялар бирга ишлашга келишиб, бир-бирларига тармоқларини очишганида, улар янги шерикларининг фақат маълум ахборотдан фойдаланишларига йўл қўйишлари лозим. Бунда конфиденциал ахборот рухсатсиз фойдаланишдан ишончли ҳимояланиши зарур. Айнан, шу сабабли корпорацияларо тармоқларда очиқ тармоқ томонидан

тармоқлараро экран (брандмауэр) ёрдамида назоратга катта аҳамият берилади. Ахборотдан ҳақиқий фойдаланувчининг фойдаланишини кафолатловчи аутентификациялаш ҳам муҳим ҳисобланади. Шу билан бир қаторда рухсатсиз фойдаланишдан ҳимоялашнинг сафланган тизими ўзига эътиборни жалб қилмаслиги шарт.

Extranet VPN уланишлари intranet VPN ва remote access VPN лар амалга оширилишидаги ишлатилган архитектура ва протоколлардан фойдаланиб сафланади. Асосий фарқ шундан иборатки, extranet VPN фойдаланувчиларига бериладиган фойдаланишга рухсат улар шеригининг тармоғи билан боғлиқ.

Баъзида VPN тармоғининг локал варианти (Localnet VPN) алоҳида гуруҳга ажратилади. Localnet VPN локал тармоғи компания локал тармоғи ичида (одатда, марказий офис) айланувчи ахборотлар оқимидан компаниядан ишловчи "ортиқча қизиқувчи" ходимларнинг рухсатсиз фойдаланишидан ҳимоялашни таъминлайди. Таъкидлаш лозимки, ҳозирда VPNни амалга оширувчи турли усулларнинг конвергенцияси ғояси кўзга ташланмоқда.

Техник амалга ошириш бўйича VPNнинг туркумланиши. Виртуал хусусий тармоқнинг конфигурацияси ва характеристикалари кўп жиҳатдан ишлатиладиган VPN-қурилмаларининг турига боғлиқ.

Техник амалга ошириш бўйича VPNнинг қуйидаги гуруҳлари фарқланади:

- маршрутизаторлар асосидаги VPN;
- тармоқлараро экранлар асосидаги VPN;
- дастурий таъминот асосидаги VPN;
- ихтисослаштирилган аппарат воситалари асосидаги VPN.

Маршрутизаторлар асосидаги VPN. VPN қуришнинг ушбу усулига биноан ҳимояланган каналларни яратишда маршрутизаторлардан фойдаланилади. Локал тармоқдан чиқувчи барча ахборот маршрутизатор орқали ўтганлиги сабабли, унга шифрлаш вазифасини юклаш табиий. Маршрутизатор асосидаги VPN асбоб-ускуналарига мисол тариқасида Cisco-Systems компаниясининг қурилмаларини кўрсатиш мумкин.

Тармоқлараро экранлар асосидаги VPN. Аксарият ишлаб чиқарувчиларнинг тармоқлараро экрани туннеллаш ва маълумотларни шифрлаш вазифаларини мададлайди. Тармоқлараро экранлар асосидаги ечимга мисол тариқасида Check Point Software Technologies компаниясининг Fire Wall-1 маҳсулотини кўрсатиш мумкин. Шахсий компьютер асосидаги тармоқлараро экранлар фақат узатилувчи ахборот ҳажми нисбатан кичик бўлган тармоқларда қўлланилади. Ушбу усулнинг камчилиги бита ишчи ўрнига ҳисобланганда ечим нарҳининг юқорилиги ва унумдорликнинг тармоқлараро экран ишлайдиган аппарат таъминотига боғлиқлиги.

Дастурий таъминот асосидаги VPN. Дастурий усул бўйича амалга оширилган VPN маҳсулотлар унумдорлик нуқтаи назаридан ихтисослаштирилган қурилмадан қолишсада, VPN-тармоқларни амалга оширилишида етарли қувватга эга. Таъкидлаш лозимки, масофадан фойдаланишда зарурий ўтказиш полосасига талаблар катта эмас. Шу сабабли, дастурий маҳсулотларнинг ўзи масофадан фойдаланиш учун етарли унумдорликни таъминлайди. Дастурий маҳсулотларнинг шубҳасиз афзаллиги– қўлланилишининг мосланувчанлиги ва қулайлиги, ҳамда нархининг нисбатан юқори эмаслиги.

Ихтисослаштирилган аппарат воситалари асосидаги VPN. Ихтисослаштирилган аппарат воситалари асосидаги VPNларнинг энг муҳим афзаллиги унумдорлигининг юқорилигидир. Ихтисослаштирилган VPN тизимларда шифрлашнинг микросхемаларда амалга оширилиши тезкорликнинг таъминланишига сабаб бўлади. Ихтисослаштирилган VPN-қурилмалар хавфсизликнинг юқори даражасини таъминлайди, аммо уларнинг нарҳи анчагина юқори.

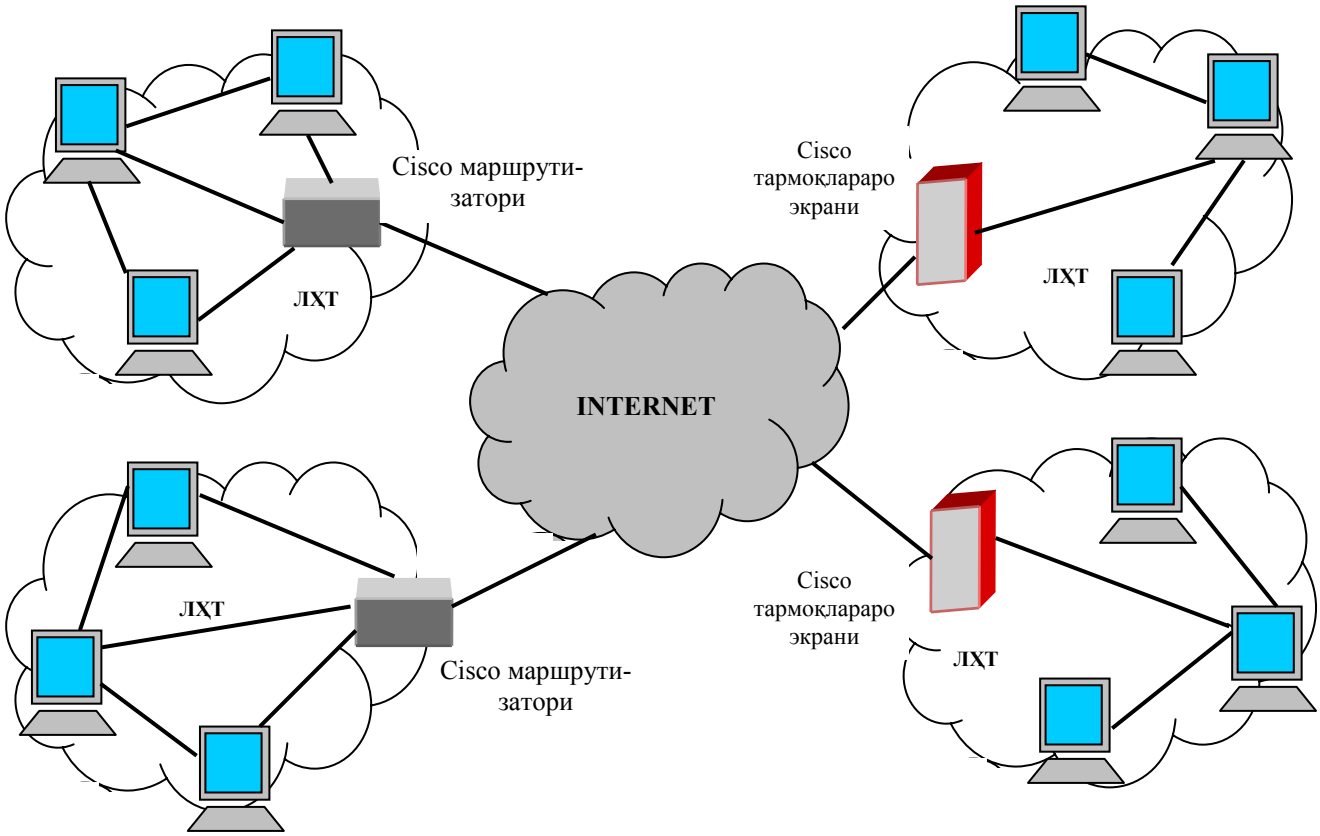
8.3. Ҳимояланган корпоратив тармоқларни қуриш учун VPN ечимлар

Маршрутизаторлар асосидаги VPN. Ташқи дунё билан локал тармоқ алмашадиган барча ахборот машрутизатор орқали ўтади. Бу маршрутизаторларни чиқувчи пакетларни шифрловчи ва кирувчи пакетларни расшифровка қилувчи табиий платформага айлантиради. Бошқача айтганда,

маршрутизатор, умуман, маршрутлаш вазифасини VPN вазифасини мададлаш билан бирга олиб бориши мумкин. Бундай ечим ўзининг афзалликлари ва камчиликларига эга. Афзаллиги – маршрутлаш ва VPN вазифаларини биргаликда маъмурлаш қулайлигидир. Корхона тармоқлараро экранни ишлатмасдан корпоратив тармоқ ҳимоясини фақат ҳам тармоқдан фойдаланиш бўйича, ҳам узатиладиган трафикни шифрлаш бўйича ҳимоялаш вазифаларини биргаликда ҳал этувчи маршрутизатор ёрдамида ташкил этган ҳолларда машрутизаторларни VPNни мададлашда ишлатилиши айниқса фойдалидур. Ушбу ечимнинг камчилиги маршрутлаш бўйича асосий амалларнинг трафикни кўп меҳнат сарфини талаб этувчи шифрлаш ва аутентификациялаш амаллари билан бирга олиб борилиши натижасида маршрутизатор унумдорлигига қуйиладиган талабларнинг ошиши билан боғлиқ. Маршрутизаторларнинг унумдорлигини оширишга шифрлаш вазифаларини аппарат мададлаш орқали эришилади. Ҳозирда барча маршрутизатор ва бошқа тармоқ қурилмаларини етакчи ишлаб чиқарувчилар ўзларининг маҳсулотларида турли VPN-протоколларини мададлайдилар. Бу соҳада Cisco Systems ва 3Com компаниялари лидер ҳисобланадилар. Cisco Systems компанияси ўзлари ишлаб чиққан маршрутизаторларга энг кенг тарқалган стандартлар асосида VPNларни қуришга имкон берувчи канал сатҳи протоколини мададловчи IOS 11.3(Internetwork Operation System 11.3) ва тармоқ сатҳи протоколи IPSecни киритди. L2F протоколи аввалроқ IOS операцион тизимнинг компонентига айланди ва Cisco ишлаб чиқарадиган барча тармоқлараро алоқа ва масофадан фойдаланиш қурилмаларида мададланади.

Cisco маршрутизиторларида VPN вазифалари бутунлай дастурий йўл билан ёки шифрлаш сопроцессори бўлган махсус кенгайтириш платасидан фойдаланилган ҳолда амалга оширилиши мумкин. Охирги вариант VPN амалларида маршрутизатор унумдорлигини анчагина оширади. Cisco Systems компанияси томонидан ишлаб чиқилган VPN қуриш технологияси юқори унумдорлиги ва мосланувчанлиги билан ажралиб туради. Унда "тоза" ёки инкапсуляция қилинган кўринишда узатилувчи ҳар қандай IP-оқим учун шифрлаш билан туннеллаш таъминланади. Cisco компаниясининг маршрутизаторлари асосида VPN-каналларини қуриш операционтизимининг

воситалари ёрдамида Cisco IOS 12.x. версиясидан бошлаб амалга оширилади. Агар мазкур операцион тизим компаниянинг бошқа бўлимларидаги Cisco чегара маршрутизаторларида ўрнатилган бўлса, бир маршрутизатордан иккинчисига "нуқта-нуқта" туридаги виртуал ҳимояланган туннеллар мажмуасидан иборат бўлган корпоратив VPN тармоқни шакллантириш имконияти бўлади (8.7-расм).



8.7-расм. Cisco маршрутизаторлари асосида корпоратив VPN тармоғини қуришнинг намунавий схемаси.

Маршрутизаторлар асосида VPNларни қуришда эсда тутиш лозимки, бундай ёндашишнинг ўзи компаниянинг умумий ахборот хавфсизлигини таъминлаш муаммосини ҳал этмайди, чунки барча ички ахборот ресурслар барибир ташқаридан хужум қилиш учун очиқ қолади. Бу ресурсларни ҳимоялаш учун, одатда, чегара маршрутизаторларидан кейин жойлашган тармоқлараро экранлардан фойдаланилади.

Cisco 1720 VPN Access Router маршрутизатори катта бўлмаган ва ўртача корхоналарда ҳимояланган фойдаланишини ташкил этишга аталган.

Бу маршрутизатор Internet ва интратармоқлардан фойдаланишни ташкил этишга зарур бўлган имкониятларни таъминлайди ва Cisco IOS дастурий таъминот асосидаги виртуал хусусий тармоқларни ташкил этиш вазифаларини мададлайди. Cisco IOS операцион тизими маълумотларни ҳимоялаш, хизмат сифатини бошқариш ва юқори ишончилиликни таъминлаш бўйича VPN вазифаларининг жуда кенг тўпламини таъминлайди.

Cisco 1720 маршрутизатори маълумотлар ҳимоясининг қуйидаги вазифаларини бажаради:

- *тармоқлараро экранлаш.* Cisco IOS Firewall компонента локал тармоқларни хужумлардан ҳимоялайди. *Фойдаланишнинг контекстли назорати* CBAC (Context-based access control) функцияси маълумотларни динамик ёки холатларга асосланган, иловалар бўйича дифференциалланган фильтрлашни бажаради. Бу функция самарали тармоқлараро экранлаш учун жуда муҳим ҳисобланади. Cisco IOS Firewall компонента қатор бошқа фойдали вазифаларни ҳам, хусусан, "хизмат қилишдан воз кечиш" каби хужумларни аниқлаш ва олдини олиш, Javani блокировка этиш, аудит ва вақтнинг реал масштабида огоҳлантиришларни тарқатиш вазифаларини бажаради.

- *шифрлаш.* IPSec протоколидаги DES ва Triple DES шифрлаш алгоритмларини мададлаш маълумотларни конфиденциаллиги ва яхлитлигини ва маълумотлар манбаини аутентификациялашни (маълумотлар глобал тармоқдан ўтганидан сўнг) таъминлаш мақсадида ишончли ва стандарт шифрлайди.

- *туннеллаш.* Туннеллашнинг IPSec, GRE (Generic Routing Encapsulation), L2F ва L2TP стандартлари ишлатилади. L2F ва L2TP стандартлари масофадаги фойдаланувчиларнинг корхона локал тармоғида ўрнатилган Cisco 1720 маршрутизаторгача виртуал туннел ўтказганларида ишлатилади. Бундай қўлланишда корхонада масофадан фойдаланиш серверига эҳтиёж қолмайди ва шаҳарлараро ёки халқаро қўнғироқлар учун тўлови тежалади.

- *қурилмаларни аутентификациялаш ва калитларни бошқариш.* IPSec катта тармоқларда маълумотлар ва қурилмаларни масштабланувчи аутентификациялашни таъминловчи калитларни бошқариш протоколи IKE,

рақамли сертификатлар X.509 версия 3, сертификатларни бошқарувчи протокол CEP, ҳамда Verisign ва Entrust компания сертификат серверлари мададланади.

- *VPNнинг мижоз дастурий таъминоти.* IPSec ва L2TP протоколларининг стандарт версиялари билан ишловчи ҳарқандай мижоз Cisco IOSбилан ўзаро алоқа қилиши мумкин.

- *фойдаланувчиларни аутентификациялаш.* Бунинг учун PAP, CHAP протокллари, TACACS^{+} ва RADIUS тизимлари, фойдаланиш токенлари каби воситалардан фойдаланилида.

Виртуал ҳимояланган тармоқлар нафақат маълумотларни ҳимоялаш, балки ҳимоялашнинг юқори савияси QoSни (Quality of Service) таъминлаши лозим. Cisco 1720 маршрутизатори QoSни қуйидаги бошқариш механизмларини мададлайди:

- *фойдаланишнинг келишилган тезлиги CAR* (Committed Access Rate) иловалар ёки фойдаланувчилар базисида қуийдаги учта муҳим вазифани бажаради:

  - трафик турини туркумлайди;
  - берилган иловага рухсат этилган ўтказиш қобилиятининг максимал даражасини ўрнатади;
  - трафикнинг ҳар бир тури устиворлигини белгилайди;

- *сиёсат асосида маршрутлаш* (Policy Routing) ҳам трафикни туркумлайди ва устиворлайди ҳамда трафикнинг қайси турини маршрутизаторнинг мос чиқиш йўли портига жўнатиш лозимлигини ҳал этади;

- *мулоҳазали одилона навбат* WFQ (Weighted Fair Queneing) трафикни ҳисобга олган ҳолда мақбул жавоб вақтини таъминлайди;

- *протокол RSVP* иловаларга йўлнинг бошидан охиригача кафолатланган ўтказиш қобилиятини резервлашга имкон беради.

Маршрутизаторнинг мослашувчанлиги модулли конструкция ва иккита слотда ўрнатилувчи интерфейс WAN-карталари тўплами орқали таъминланади. Cisco 1720 моделида Cisco 1600, 2800, ва 3600 моделларда ишлатиладиган WAN-карталардан фойдаланилади.

Компания 3Com VPN технологияни амалга оширишда бошидан стандартларни кўзга тутган эди. VPN ни мададлаш унинг NetBuilder II, Super Stack II NetBuilder маршрутизаторларига Office Connect Net Builder Platform ларида ўрнатилган.

3Com компанияси PPTP ва L2TP протоколларни мададловчи масофадан фойдаланилувчи концентраторларни йирик ишлаб чиқарувчиларидан биридир. 3Com компаниясининг VPN тармоқлари IPSec билан бирга ишлатилади ва ташқи каталоглар, жумладан Novell NDS ва Windows NT Directory Servicesлар билан ўзаро алоқа қилиш учун ишлаб чиқилган.

Компания Web-технологияга асосланган ва VPN юкланганлигини назоратлашга, ҳамда юз берувчи ходисалар асосида статистика ва ахборотни йиғишга аталган дастурий илова Transcend Ware Secure VPN Manager ни ҳам ишлаб чиқди. Ундан ташқари 3Com криптоҳимояланган туннелларни осонгина яратишга имкон берувчи Web асосидаги инструментарийни ишлаб чиқаради.

Internet Devices компаниясининг Fort Knox маршрутизаторларида тезлик ва қувват уйғунлашган. Ундаги тармоқни ҳимоялашни таъминлашга йўналтирилган IP-трафикни ишлаш вазифалари руйхатининг кенглиги унинг афзаллигидир. Fort Knox маршрутизатори тармоқлараро экран режимида ишлаши, NAT стандарти бўйича адресларни трансляциялаши, хавфсизлик сиёсатини бошқариши, Web-саҳифалар ва DNS жадвал ёзувларини кэшлаши, аудитни бажариши мумкин. Одатда Fort Knox корпоратив тармоқ чегарасида, корпоратив тармоқни глобал тармоқ билан уловчи маршрутизатордан кейин ўрнатилади. Демак, у бошқа локал тармоқлар билан VPN-алоқани ўрнатиш ва тармоқлараро экранлар каби фойдаланишни назоратлашнинг турли қоидаларини шакллантириши мумкин. Fort Knoxда NAT адресларини трансляциялаш функциясининг мавжудлиги, унга ички IP-адресларни беркитиш ва маршрутизаторлар трафигини қайта йўналтириш имконини беради. Бу корпоратив тармоқ маъмурларини VPNни қуришда маршрутизаторларни янгидан конфигурациялашдан озод этади. Fort Knox функциялари тўпламининг кенглигига қарамай унинг нархи оддий маршрутизатор нархига тенг.

Тармоқлараро экранлар асосидаги VPN. Локал тармоқнинг тармоқлараро экрани орқали, худди маршрутизатордагидек, бутун трафик ўтади. Шу сабабли, тармоқлараро экран ҳам чиқувчи трафикни шифрлаш, кирувчи трафикни расшифровка қилиш вазифасини бажариши мумкин. Ҳозирди қатор VPN-ечимлар тармоқлараро экранларни VPNнинг қўшимча мадад функциялари билан тўлдирилишига таянади. Бу Internet орқали бошқа тармоқлараро экранлар билан шифрланган уланишни ўрнатишга имкон беради. Ахборот хавфсизлиги бўйича қатор мутахассисларнинг фикрича VPNни тармоқлараро экранлар асосида қуриш, корпоратив тармоқларни очиқ тармоқлар хужумларидан комплекс ҳимоялаш нуқтаи назаридан, тўла асосланган ечимдир. Ҳақиқатан, тармоқлараро экран ва VPN-шлюз функциялари бир нуқтада, ягона бошқариш ва аудит тизими назоратида бирлаштирилса, корпоратив тармоқни ҳимоялаш функциялари битта қурилмада тўпланади. Натижада ҳимоя воситаларини маъмурлаш сифати ошади.

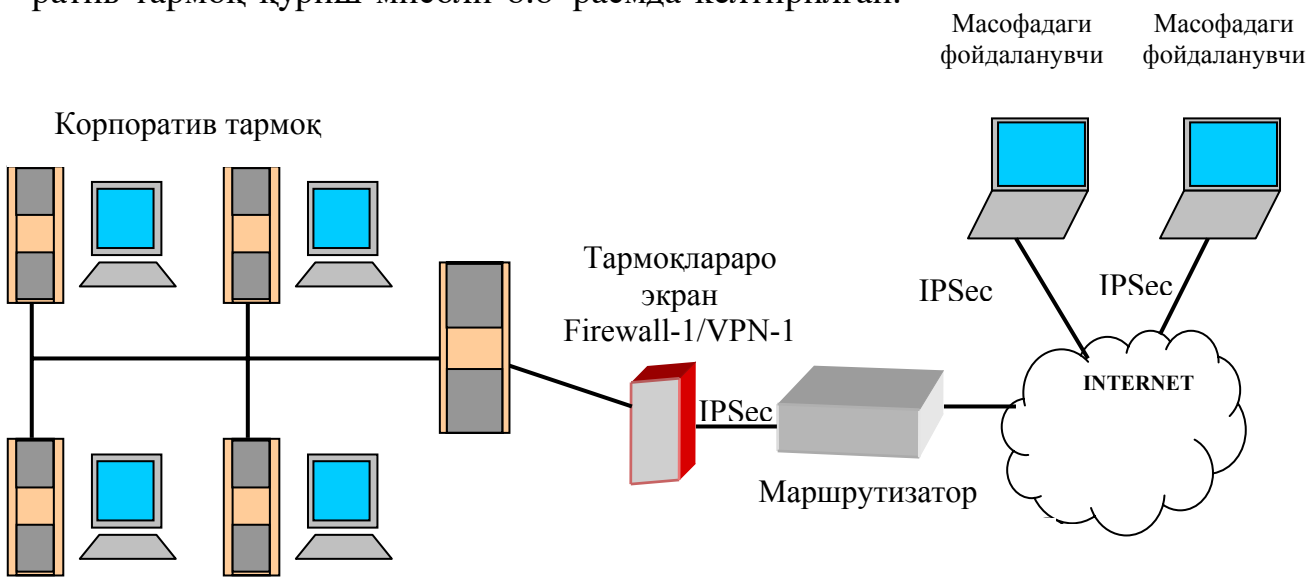
Аммо, ҳимоялаш воситаларининг бундай универсаллаштирилиши, ҳисоблаш воситаларининг мавжуд имкониятлари даражасида нафақат ижобий, балки салбий томонига ҳам эга. Шифрлаш ва аутентификациялаш амалларини ҳисоблаш мураккаблиги тармоқлараро экран учун анъанавий бўлган пакетларни фильтрлаш амалларига нисбатан анча юқори. Шу сабабли, VPNнинг қўшимча вазифаларини амалга оширишда мураккаблиги катта бўлмаган амалларни бажаришга мўлжалланган тармоқлараро экран кўпинча керакли унумдорликни таъминламайди. Корпоратив тармоқ тезкор канал орқали очиқ тармоққа уланганида сифатли ҳимояни таъминлаш учун алоҳида аппарат, дастурий ёки комбинацияланган қурилма кўринишидаги VPN-шлюздан фойдаланиш лозим.

Аксарият тармоқлараро экранлар сервер дастурий таъминотидан иборат, шу сабабли унумдорликни ошириш муаммоси юқори унумдорликка эга бўлган компьютер платформасидан фойдаланиш эвазига ечилиши мумкин.

Check Point Software Technologies компанияси Internet билан ишлаганда ахборот хавфсизлигини комплекс таъминлаш махсулотларини ишлаб чиқариш соҳасидаги етакчилардан бири ҳисобланади. Check Point Fire Wall-1 тармоқлараро экран корпоратив ахборот ресурслари учун ягона

комплекс доирасида ҳимоянинг чуқур эшелонланган чегарасини қуришга имкон беради. Бундай комплекс таркибига Check Point FW-1 нинг ўзи ва корпоратив VPN тармоқ (ҳимояланган туннеларни шакллантирувчи қисм тизим) қуриш учун маҳсулотлар тўплами Check Point VPN-1, ҳамда суқилиб киришни пайқаш воситалари Flood Gate ва ҳ. киради.

Дастурий таъминотлар Check Point Fire Wall-1/VPN-1 асосида корпоратив тармоқ қуриш мисоли 8.8–расмда келтирилган.



8.8–расм. Check Point FW-1/VPN-1 асосида корпоратив VPN тармоғини қуриш схемаси.

Check Point VPN-1 қисм тизим таркибидаги барча маҳсулотлар ҳам ўзаро, ҳам оммавий брандмауэр Fire Wall-1 билан узвий интеграцияланган. Check Point компанияси "тармоқ-тармоқ" (VPN-1 Gateway) ва "тармоқ-масофадаги фойдаланувчи" (VPN-1 Gateway+VPN-1 Secu Remote) типидаги ҳимояланган тармоқларни ташкил этиш учун воситаларни тақдим этади.

Check Point VPN-1 маҳсулотлари очиқ стандартлар (IPSec) асосида амалга оширилган, фойдаланувчиларни аутентификациялашнинг ривожланган тизимига эга, очиқ калитларни (PKI) тақсимлашнинг ташқи тизимлари билан ўзаро алоқани мададлайди, бошқариш ва аудитнинг марказлаштирилган тизимини қуришга имкон беради ва ҳ.

Check Point Fire Wall-1/VPN-1 нафақат очиқ, балки криптоҳимояланган трафикни ҳам назоратлайди. Тармоқлараро экран FW-1га келган маълумотлар VP-1 воситалари ёрдамида расшифровка қилинади, сўнгра ахборотлар пакети яна шифрланади ва ўтказиб юборилади.

VPN-1 қисм тизими трафикни нафақат криптографик беркитади, балки ахборотлар пакетини аутентификациялайди ҳам.

Check Point Fire Wall-1/VPN-1 каналларида трафикни шифрлашда машхур алгоритмлар DES, 3-Des, CAST, IDEA, FWZ1 ва ҳ. алгоритмлардан фойдаланилади. FWZ1 криптотизими Check Point компаниясининг ишланмасидир. Ахборот пакетларини аутентификациялашда MD5, SHA-1, CBC DES ва MAC алгоритмлари ишлатилади.

VPN Gateway шлюзи – шифрлашнинг дастурий модули тармоқлараро экран Fire Wall – 1 билан узвий интеграцияланган. Бу маҳсулот корхонага узатилувчи маълумотларнинг тўла конфиденциаллигини, аутентификацияланганлиги ва яхлитлигини кафолатлаган ҳолда Internet орқали алоқа каналларини қуришга имкон беради. VPN функциялари корхонанинг умумий хавфсизлик сиёсатига тўла интеграцияланганлиги сабабли, брандмауэр ва VPN-маҳсулотларни алоҳида бошқаришга эҳтиёж қолмайди.

VPN Gateway шлюзи ҳимояланган VPN-туннелни ўрнатган ҳолда тармоқлар орасида Intrenet орқали узатилаётган конфиденциал маълумотларни шифрлайди. Бу шлюз уни жавобгарлик доирасига, яъни унинг доменига кирувчи компьютерлардан келадиган маълумотлар оқимини шифрлайди. Бу локал тармоқ ёки ушбу шлюз орқасидаги оддий хостлар гуруҳи бўлиши мумкин. Бу маълумотлар тармоқнинг оммавий қисми бўйича шифрланган кўринишда узатилади, ички тармоқ бўйича узатилганда шифрланмайди. VPN-амалларининг барчаси охирги фойдаланувчи ва барча иловалар учун шаффофдир.

VPN-1 Gateway шлюзи шифрлашнинг бир неча алгоритмини ва бир неча калитларни бошқариш протоколини мададлайди. Бу шлюз IKE (Internet Key Exchange) каби индустриал стандарт VPN-протоколларни мададлаши сабабли, экстратармоқларни ташкил этишда қўллаш қулай ҳисобланади. Экстратармоқларда VPN бизнес-шериклар орасида хавфсиз алоқани таъминлайди. Check Point компаниясининг VPN-маҳсулотлари IKE стандартига амал қилади. Шу сабабли улар қарши томон билан музокаралар жараёнида автоматик тарзда шифрлашнинг энг криптобардош алгоритмини (DES ва Triple DES) ва аутентификациялашнинг энг қатъий алгоритмини

(SHA-1 ва MD5) танлайди. Ундан ташқари, шифрлашнинг махфий калитлари, максимал ҳимояланишни кафолатлаган ҳолда, тез-тез янгиланади.

VPN-1 Gateway шлюзи виртуал хусусий тармоқдаги иккита охирги узелларга ҳам шифрланган, ҳам шифрланмаган маълумотларни алмашишга имкон берувчи шифрлашнинг танлов режимини мададлайди. Бунинг учун тармоқ маъмури трафиги учун ҳимоялашнинг алоҳида шартлари таъминланадиган иловаларни беради. Сўнгра VPN-1 Gateway ушбу иловалар маълумотларини шифрланган, қолган конфиденциал бўлмаган маълумотларни очиқ кўринишда узатишни бошлайди. Бундай мосланувчанлик VPN-1 Gateway шлюзининг унумдорлигини оширади.

VPN-1 Gateway шлюзи калитларни бошқаришнинг қуйидаги механизмларини мададлайди: IPSec учун стандарт бўлган IKE, калитларни бошқаришнинг саноат стандарти FWZ, оммавий протокол SKIP ва калитларни қўл билан тарқатиладиган усули. У X.509 сертификатлари ва Entrus Technologies компаниясининг сертификатлар серверлари технологияси асосида очиқ PKI калитларни бошқариш инфратузилмасини мададлайди.

VPN-1 Secu Remote мижоз дастурий таъминоти VPN-1 Gateway Шлюзи ёрдамида "тармоқ-масофадаги фойдаланувчи" ҳилидаги ҳимояланган уланишларни ташкил этишда ишлатилади. Windows 9X/XP/NT/2000 бошқарувида ишловчи масофадаги компьютерларга VPN-1Secu Remoteнинг ўрнатилиши Мобил ходимларнинг ёки телекомпьютерларнинг корхона бош тармоғи билан Internet орқали ҳимояланган боғланишини таъминлайди. VPN-1 Secu Remoteнинг маҳсулотларни OSI моделининг тармоқ сатҳида шифрлаши ва расшифровка қилиши ушбу амалларнинг барча иловалар учун шаффофлигини, мавжуд иловаларга ўзгартириш киритишни талаб қилмаган ҳолда, таъминлайди. SecuRemote фойдаланувчиларга VPN-воситалар ўрнатилган бир неча турли тармоқлар билан боғланишига имкон беради.

VPN-1 Accelator Card қурилмаси Chrysalis-ITS компанияси томонидан ишлаб чиқилган аппарат криптографик тезлатгичдир. VPNнинг ҳимояланган каналларида трафикни шифрлаш ва калитларни генерацияловчи амаллар анчагина ҳисоблаш мураккаблигига эга ва VPN орқали узатилувчи тра-

фикнинг хажми ошган сари компьютернинг процессори ва хотирасининг хаддан ортиқ юкланиши рўй бериши мумкин. VPN-1 Accelator маҳсулоти бу муаммони ҳал этиши мумкин.

VPN-1 Accelator Card тезлатгичи VPN-1 Gateway шлюзи билан биргаликда ишлашга аталган ва IKE ва IPSeclар талаб этадиган барча криптографик амалларни бажаради. VPN-1 Accelator Card бевосита шлюз орқали маъмурланади.

VPN функциялари ўрнатилган SecureZone тармоқлараро экрани Secure Computing компанияси томонидан ишлаб чиқилган ва асосий характеристикалари қуйидагича:

- VPNни мададлаш функциялари – IPSec стандарти, DES ва Triple DES, PKI бошқариш ва Netscape, Entrust ва Verisign компаниялардан X.509 сертификатлари;

- ихтисослаштирилган операцион тизими Secure OS (Unixнинг ҳимояланган варианти) бошқарувида ишлайди;

- қуйидагиларни қаноатлантирувчи аппарат платформалар: процессор Intel Pentium, Pentium Pro, ёки Pentium II; RAM-камида 64Мбайт; ташқи қурилмалар қаттиқ диск 4 Гбайт SCSI-2, қайишқоқ дисклар 3,5", COKOM, стриммер DAT; SVGA video, PS/2- билан бирга ишлай олувчи сичқон.

- стандарт тармоқ интерфейслари: 2-4 Ethernet, FAST Ethernet, Token Ring ёки FDDI;

- бузилишга бардошлик хоссасига эга.

Secure Computing компанияси MicroSoft Windows муҳитида ишловчи, алоҳида фойдалунувчиларга TCP/IP протоколлари бўйича телефон тармоғи ёки пакетларни коммутацияловчи, оммавий тармоқдан ҳимояланган масофавий фойдаланишни таъминловчи, IPSec билан бирга ишлайолувчи мижоз дастурий таъминотини (SecureClient) ҳам тавсия этади.

VPN функциялари ўрнатилган Raptor Firewall 5.0 тармоқлараро экрани Axent Technologies компанияси томонидан ишлаб чиқилган ва Eagle Firewallнинг модификацияланган маҳсулоти ҳисобланади. Бу тармоқлараро экраннинг характеристикалари қуйидагича:

- VPN мадади тармоқлараро экранга ўрнатилган;

- IPSec стандарти мададланади, дастурий шифрлаш IP (текин тарқатилувчи шифрлаш усули swIPe);

- хавфсизликнинг умумий сиёсати тармоқлараро экран функцияларига ва VPN функцияси ёрдамида туннелланувчи трафикка тааллуқли;

- Windows NT/2000 ва Solaris операцион тизимлар бошқарувида ишлайди.

Axent компанияси масофадаги фойдаланувчилар учун VPNнинг мижоз дастурий таъминотини ҳам тақдим этади. Raptor Firewall 5.0 версияси IPSec протоколи бўйича ҳимояланган виртуал тармоқ қурилишини таъминлайди.

Gauntlet Global VPN маҳсулоти Network Associates компанияси таркибига кирувчи Trusted Information Systems компаниясининг Gauntlet Firewall тармоқлараро экрани учун, ушбу тармоқлараро экран муҳитида узвий интеграцияланувчи, қўшимча дастурий маҳсулот ҳисобланади.

IPSec протоколига асосланган Gauntlet Global VPN қисм тизими трафикни криптографик ҳимоялашнинг қуйидаги иккита режимини мададлайди:

- Smart Gate шлюзлари ёрдамида амалга оширилувчи тармоқлараро экрандан тармоқлараро экрангача;
- масофадаги мижоз дастурий таъминоти Gauntlet PC Extender ёрдамида амалга оширилувчи тармоқлараро экрандан масофадаги фойдаланувчи компьютеригача.

Gauntlet Global VPNда шифрлашнинг DES алгоритми ишлатилади. Gauntlet Global VPN сертификация марказининг дастурий таъминоти билан ҳам тақдим этилади. Ушбу дастурий таъминот ёрдамида ташкилотлар X.509 стандартига мос келувчи рақамли сертификатларни генерациялаши ва текшириши мумкин.

VPN қуриш функциясини мададловчи BorderManager тармоқлараро экрани Novell компаниясининг маҳсулоти бўлиб, нафақат VPN қуриш имкониятини, балки фойдаланишни чегаралашни, пакетларни фильтрлаш ва тармоқ адресларини трансляциялашни таъминлайди, воситачи HTTPнинг хизматларини тавсия этади, Web саҳифаларини кешлайди, канал сатҳида

шлюзларга эга, кўп протоколли маршрутлашни бажаради ва масофадан фойдаланишни мададлайди.

Border Manager тармоқлараро экраннинг NDS (Novell Directory Service) каталоглари хизмати билан узвий интеграцияси ҳимояланган виртуал тармоқларни самарали бошқаришга имкон беради. Шифрлаш калитининг тақсимоти RSA криптотизими ва Диффи-Хеллман алгоритми бўйича амалга оширилади. Ахборот пакетларини криптографик беркитиш ва аутентификациялашда RC2 ва RSA криптотизимлардан фойдаланилади. Border Managerнинг бир версиясида IPSec протоколи мададланади. Border Manager тармоқлараро экран асосида қурилган ҳимояланган виртуал тармоқларда брандмауэрлардан бирининг асосий бўлиши, бошқариш маркази ролини бажариши лозим.

Ихтисослаштирилган дастурий таъминот асосидаги VPN. VPN қуришда ихтисослаштирилган дастурий воситалар кенг қўлланилади. VPN қуришнинг дастурий воситалари ҳимояланган туннелларни фақат дастурий шакллантиришга имкон беради ва улар ишлайдиган компьютерни TCP/IP маршрутизаторига айлантиради. Бу маршрутизатор шифрланган пакетларни қабул қилади, расшифровка қилади ва локал тармоқ орқали тайинланган нуқтага узатади. Охирги вақтда бундай маҳсулотларнинг етарлича сони пайдо бўлди. Ихтисослаштирилган дастурий таъминот кўринишида VPN-шлюзлар, VPN-серверлар ва VPN-мижозлар бажарилиши мумкин.

Дастурий усул бўйича амалга оширилган VPN-маҳсулотлар унумдорлик нуқтаи-назаридан ихтисослаштирилган аппарат қурилмалардан қолишсада, дастурий маҳсулотлар масофадаги фойдаланувчиларга етарли унумдорликни осонгина таъминлайди. Дастурий маъсулотларнинг шубҳасиз афзаллиги ишлатилишида мосланувчанлиги ва қулайлиги, ҳамда нисбатан юқори бўлмаган нархидир. Аппарат шлюзларни ишлаб чиқарувчи кўпгина компаниялар (масалан, Time Step, VPNet, Shiva) ўзларининг маҳсулотларига стандарт операцион тизимда ишлашга мўлжалланган VPN-мижознинг дастурий амалга оширилишини қўшадилар.

MicroSoft компаниясининг RAS ва RRAS дастурий маҳсулотлари. MicroSoft компаниясининг масофадан фойдаланувчи дастурий сервери RAS

(Remote Access Service) машҳур PPP (Point to Point Protocol) протоколнинг кенгайтирилган варианти-ҳимояланган канал протоколи PPTPни (Point-to-Point Tunneling Protocol) ўрнатилиши эвазига VPN технологияни мададлайди. Трафикни туннеллаш очиқ IP-тармоқ бўйича узатиладиган стандарт PPP- фреймларни IP-датаграммаларга инкапсуляциялаш ва кейин шифрлаш орқали амалга оширилади.

RASнинг асосий афзаллиги – тежамлилиги, камчилиги - унумдорлигининг пастлиги. Ҳозирда бу маҳсулотнинг такомиллаштирилган версияси – RRAS (Routing and Remote Acces Service) пайдо бўлди. RRAS таркибидаги такомиллаштирилган дастурий кўп протоколли маршрутизатор маршрутлашнинг RIP (Routing Information Protocol) ва OSFP (Open Shortest Path First) протоколларини мададлайди. RRASнинг бу хусусиятлари ундан VPN шлюзи каби "тармоқ-тармоқ" ўзаро алоқасида фойдаланишга имкон яратади. RAS хизмати масофадан фойдаланувчиларнинг кўпчилигига (256 тагача) битта Windows NT серверига уланиш ва локал тармоқ ресурсларидан IPX ва TCP/IP протоколлари бўйича фойдаланиш имкониятини беради.

Alta Vista Tunnel 98 маҳсулотлари оиласи учта маҳсулотни ўз ичига олади: Telecommuter Server, Extranet Server, AltaVista Tunnel Client. Telecommuter Server сервери Internet корпоратив фойдаланувчилар орасида ҳимояланган туннеларни Internet орқали ташкил этишга аталган. Extranet Server сервери ёрдамида тармоқлар орасида ҳимояланган канални ҳосил қилинади. Бу иккала сервер умумий Alta Vista Tunnel Server номига эга. Alta Vista Tunnel Client VPN клиентнинг дастурий таъминотидир.

Alta Vista Tunnel 98 оиласининг барча маҳсулотлари фойдаланувчиларни аутентификациялашда ва RSA криптографик тизимнинг сессия калитларини алмашишда ишлатилади. Фойдаланувчиларни аутентификациялашда Security Dynamics компаниясининг аппарат калити SecurID ҳам ишлатилиши мумкин. Мижоз ва сервер янги сессия калитлари билан ҳар 30 минутда алмашишади.

Маълумотларни шифрлашда RC4 алгоритмидан фойдаланилади. Маҳсулотларнинг ҳалқаро версияси RC4 алгоритми бўйича шифрлашда 56 ёки 4 битли калитлардан фойдаланади. Маълумотларни аутентификациялаш

ва яхлитлигини таъминлаш учун MD5 хэш-функцияси ишлатилади. Alta Vista Tunnel 98 оиласининг маҳсулотлари LZO алгоритми бўйича маълумотларни зичлаштириши мумкин.

Ушбу оила маҳсулотлари аксарият замонавий операцион тизимлар - Windows NT/2000, Unix BSD/OS, Unix BSD ва Digital UNIX бошқарувида ишлаши мумкин. Windows NT/2000 операцион муҳитда Alta Vista Tunnel Server маҳсулоти бир вақтнинг ўзида 200 туннел уланишларини, UNIX операцион муҳитда эса 2000гача туннел уланишларни мададлайди.

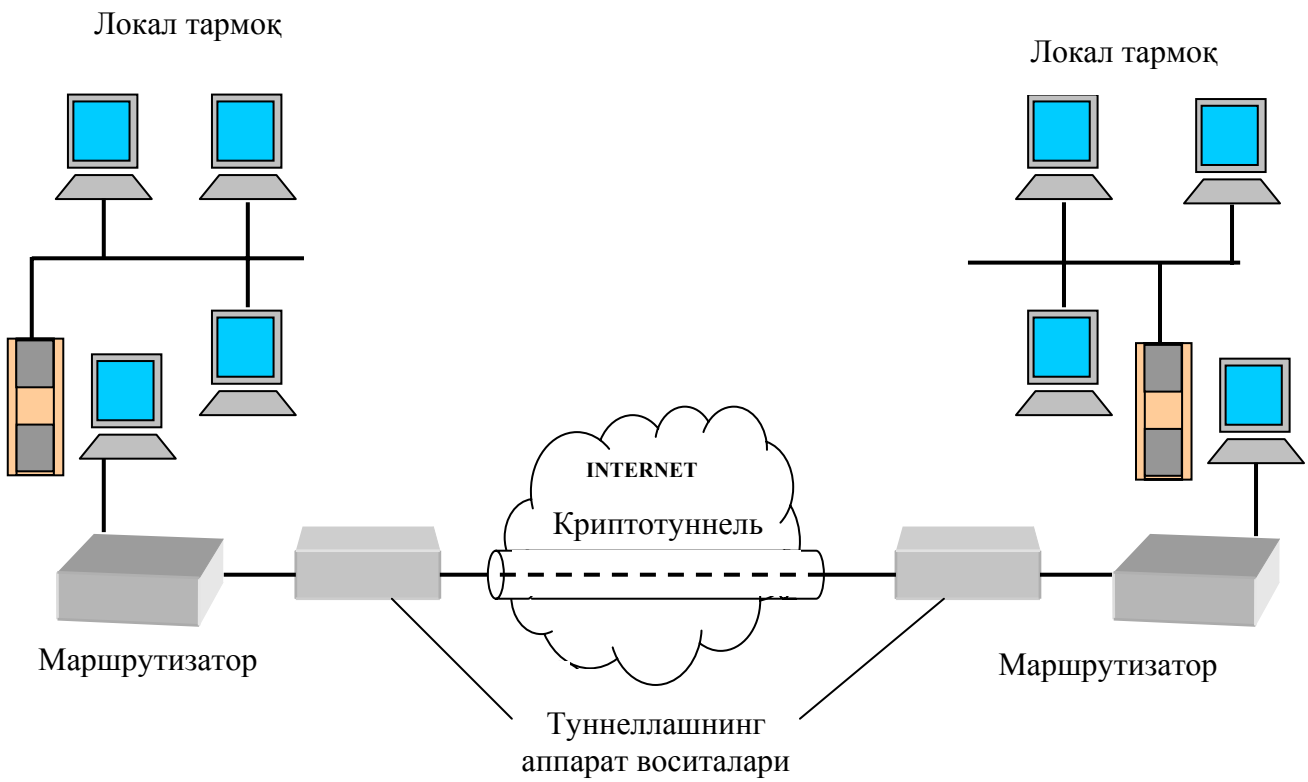
Ихтисослаштирилган аппарат воситалари асосидаги VPN. Ихтисослаштирилган аппарат қурилмалари асосидаги VPN-воситаларнинг асосий афзаллиги-юқори унумдорлиги. VPN-пакетларни ишлашда керакли ҳисоблашлар хажми оддий пакетларни ишлашдагига нисбатан 50-100 марта ошади. Аппарат воситалари асосидаги VPNларда юқори тезликка уларда шифрлашнинг ихтисослаштирилган микросхемаларда амалга оширилиши эвазига эришилади. Бундай VPN-воситалар кўпинча IPSec протоколи билан бирга ишлайолади ва локал тармоқлар орасида криптоҳимояланган туннелларни шакллантиришда ишлатилади. Баъзи ишлаб чиқарувчиларнинг VPNни шакллантирувчи асбоб-ускуналари бир вақтнинг ўзида "масофадаги компьютер-локал тармоқ" режимида ҳимояланган боғланишни ҳам мададлайди.

Аппарат VPN-шлюзлар алоҳида аппарат қурилмаси кўринишида бўлади. Уларнинг асосий вазифаси – трафикни юқори унумдорлик билан шифрлаш. Бу VPN-шлюзлар X.509 рақамли сертификатлари PKI очиқ калитларни бошқариш инфратузилмалари билан ишлайди, LDAP бўйича маълумот берадиган хизматлар билан ишлашни мададлайди.

Аппарат ҳимояланган туннел ишлашининг энг оддий варианти - аппарат шифрлашдан фойдаланиб уланишларни яратиш. Туннеллашнинг аппарат воситалари одатда локал ва глобал тармоқларнинг туташган жойида, маршрутизатордан кейин ўрнатилади (8.9-расм) ва автоматик тарзда берилган трафикни шифрлайди. Бундай ёндашишнинг асосий афзаллиги шундаки, ишчи станциялар ва маршрутизаторларнинг шакллантирилувчи крипто-

туннеллар билан ҳеч қандай боғлиқлиги йўқ, VPN ўрнатилганида уларни конфигурациясини ўзгартириш талаб этилмайди.

Аппарат шлюзларни инсталляциялаш дастурий шлюзлар ва маршрутизаторлар ва брандмауэрлар асосидаги шлюзларга нисбатан жуда осон амалга оширилади. Бундай қурилмаларни бошқариш иккита асосий масалани ечишни талаб этади: сертификация маркази орқали калитларни бошқариш ва ҳимояланган туннеллашни бошқариш. Аксарият аппарат туннеллаш воситаларида сертификация марказлари Windowsга мослашган дастурий иловалардир. Аппарат туннелларини марказлашган ҳолда бита иш жойида туриб бошқариш мумкин. Бошқарувчи дастурлар туннелнинг асосий ҳимоялаш функцияларининг бажарилишини ва хатоликларни ишлашни таъминлайди.



8.9–расм. Ихтисослаштирилган аппарат воситалар асосида туннеллаш схемаси.

Ихтисослаштирилган аппарат VPN-воситалар нархидан ташқари барча бўлиши мумкин бўлган кўрсаткичлари бўйича лидер ҳисобланади.

TimeStep компанияси корхоналарда кенг масштабли ахборот алмашинуви учун IPSec билан бирга ишлайолувчи PERMIT Enterprise Snite деб аталувчи VPN-маҳсулотни ишлаб чиқди. Ушбу маҳсулот Internet орқали ма-

софадан фойдаланишни ташкил этиш, корпоратив интратармоқ ва экстратармоқларни қуриш учун тўлиқ ечим ҳисобланади. PERMIT Enterprise мавжуд тармоқларда тармоқ ва охирги фойдаланувчи унумдорлигига жиддий таъсир қилмаган ҳолда, осонгина сафланади, унинг масштабланувчи архитектураси бирнеча VPNларни яратиш ва уларни бошқариш имкониятини беради.

Компания томонидан шлюзнинг қуйидаги тўртта модификацияси тақдим этилади:

- PERMIT/Gate 1520 нархи қиммат бўлмаган автоном қурилма бўлиб, қувватли телекомпьютерлар ёки SOHO синфидаги катта бўлмаган офислар учун ишлатилади;

- PERMIT/Gate 2520 ва PERMIT/Gate 4520 ўтказиш қобилияти, мос ҳолда 4 ва 1- Мбит/с, бўлинмалар офислари ва кичик локал ҳисоблаш тармоқларига мўлжалланган, масофадаги юзлаб фойдаланувчиларни мададлайди;

- PERMIT/Gate 7520 (70 Мбит/с) ички локал ҳисоблаш тармоқларида ишлатилади ва масофадаги минглаб фойдаланувчиларни мададлайди.

PERMIT/Gate шлюзларининг муҳим афзаллиги - трафик ишланишининг юқори унумдорлигини таъминлш мақсадида DES ва 3-DES шифрлаш алгоритмининг аппарат амалга оширилиши.

PERMIT/Gate7520 шлюзи IPSecнинг амалга оширилишининг аппарат воситаси билан ҳам жиҳозланганлиги, унумдорликка таъсир қилмаган ҳолда минглаб VPN уланишларни мададлашга имкон беради. Бу, зарурият туғилганда, корпоратив тармоқни осонгина кенгайтириш имконини яратади.

Мижоз дастурий таъминоти PERMIT/Client IPSec протоколини мададлайди ва масофадаги фойдаланувчиларга ўзининг тармоғи билан хавфсиз боғланиш имконини беради. Ушбу дастурий таъминот Windows95/98/XP/NT ёки MAC OS 7.1. бошқарувида ишловчи алоҳида ишчи станция томонидан адресланган тармоқ трафигини ҳимоялайди.

PERMIT/Gate шлюзларининг ҳар бири дастурли утилита PERMIT/Config билан бирга тақдим этилади. Бу дастурли утилита виртуал хусусий тармоқнинг ҳар қандай нуқтасидан бир неча шлюзларнинг дасту-

рий таъминотини масофадан конфигурациялаш, бошқариш ва модиифкациялашга имкон яратади.

VPNet компанияси VPN қуриш учун дастлабки интеграцияланган ечимлардан бири - VPNwareни таклиф этди. Бу ечим ўз ичига қуйидаги маҳсулотларни олади:

- учта VPN-шлюз: штаб қароргоҳи ва йирик локал тармоқлар учун VSU.1100, бўлинмалар учун VSU-1010 ва катта бўлмаган офислар учун VSU-10;

- iPass компаниясидан дастурий сервер RoamServer;

- мижоз дастурий таъминоти VPNremote;

- бошқаришнинг дастурий тизими VPNmanager.

VPNet асбоб-ускуналари, "тармоқ-тармоқ" ва "тармоқ – масофадаги фойдаланувчи" хилидаги уланишларга мўлжалланган VPNни мададлайди. Ишлатиладиган маҳсулотларга боғлиқ ҳолда VPNware тизими IPSecнинг стандарт амалга оширилиши ёрдамида оммавий IP тармоқ орқали узатилаётган маълумотларни ҳимоялаш билан 25дан 5000тача фойдаланувчиларни мададлаши мумкин. Бу тизим турли масштабли тармоқларда йирик корхонанинг марказий локал тармоғида, бўлинма ва катта бўлмаган офис локал тармоғида ва масофадаги фойдаланувчиларни ҳимоялашда ишлатилиши мумкин.

VSU-1010 ва VSU-10 шлюзлар IPSec билан бирга ишлай олади ва DES ва 3-DES алгоритмлари бўйича маълумотларни шифрлашни аппарат мададлашга эга. VPNнинг бошқарувчи иловаси статистикани йиғишга ва VPNдаги ходисаларни қайдлашга имкон беради. Ҳар хил VPNларни бошқаришни марказлаштириш эвазига ҳимояни бошқаришнинг бошқа функцияларини соддалаштириш ва марказлаштириш, масалан, корпоратив браднмауэр яхлитлигини бузилишини назоратини таъминлаш мумкин. VPNet маҳсулотларининг афзаллиги-мавжуд тармоқ билан интеграцияланишининг соддалиги, унумдорлигининг нисбатан юқорилиги ва IPSecнинг тўла амалга оширилиши.

Мижоз дастурий таъминоти VPNremote IPSec протоколини мададлайди ва Windows NT муҳитида ҳамда телефон тармоқлари орқали фойдала-

нилганда масофадаги ва мобил фойдаланувчилар, телекомпьютерлар ва бизнес-шерикларнинг маълумотларини ҳимоялашда Windows95/98/XP муҳитида ишлайди.

Бошқарув тизими VPNmanager виртуал хусусий тармоқларни яратиш, конфигурациялаш ва бошқариш учун махсус ишлаб чиқилган. Тармоқ маъмури ушбу тизим ёрдамида, график интерфейсни ишлатиб масофадаги фойдаланувчиларни ва бизнес-шерикларни VPNга осонгина қўшиши мумкин. VPN мижозларини масофадан маъмурлашга Dyna-Policy функцияси аталган.

LanRover VPN Gateway шлюзи Shiva компанияси тоомнидан тақдим этилган бўлиб, ICSA томонидан сертификацияланган. Бу шлюз очиқ тармоқ орқали узатиладиган маълумотларни ҳимоялаш технологияларининг кенг тўпламини мададлайди. Яхлитликни ва конфиденциалликни таъминлаш, фойдаланишнинг назорати, X.509нинг рақамли сертификатларига, Security Dynamics аппарат калитларига, RADIUS протоколи ёки доменли схемага асосланган аутентификациялашнинг турли схемалари бу тўпламга киради.

Маълумотларни аппарат шифрлаш DES ёки 3-DES алгоритмлари асосида амалга оширилади. LanRover VPN Gateway шлюзлари Pentium-технологиянинг тезлиги, шифрловчи ихтисослаштирилган интеграл схемаларининг тезкорлиги ва реал вақтнинг кўп вазифали операцион тизимнинг реактивлигининг ноёб бирикмасидан фойдаланади. Бу шлюзлар ишлатишда қулай ва уларнинг ишлаши охирги фойдаланувчилар учун шаффоф. Бу шлюзлар билан ишлаш қулайлигини таъминлаш мақсадида график фойдаланувчи интерфейсли утилита VPN manager тақдим этилади. Бу утилита маъмурга ҳар қандай Windows 95/NT тизимидан бирданига бир неча шлюзларни бошқаришни таъминлайди.

8.4. Канал ва сеанс сатҳларда ҳимояланган виртуал каналларни қуриш

Канал сатҳида ҳимояланган виртуал каналларни шакллантириш протоколлари.

PPTP, L2F ва L2TP протоколлар OSI модели канал сатҳининг туннеллаш протоколлари ҳисобланади. Ушбу протоколларнинг умумий хусусияти шундан иборатки, улар очиқ тармоқ, масалан Internet орқали корпоратив тармоқ ресурсларидан ҳимояланган кўп протоколли масофадан фойдаланишни ташкил этишда ишлатилади. Уччала протоколни, одатда, ҳимояланган канални шакллантириш протоколларига мансуб деб ҳисоблайдилар. Аммо бу таърифга узатиладиган маълумотларни туннеллашни ва шифрлашни таъминловчи фақат PPTP протоколи аниқ мос келади, чунки L2F ва L2TP протоколлар фақат туннеллаш функцияларини мададлайди. Туннелланган маълумотларни ҳимоялаш (шифрлаш, яхлитлик, аутентифкация) учун бу протоколларда қўшимча, протокол, хусусан IPSec протоколи ишлатилади.

PPTP протоколи маълумотларни IP, IPX ва NetBEUI протоколлари бўйича алмашиш учун ҳимояланган каналларни яратишга имкон беради. Ушбу протоколлар маълумотлари PPP кадрларига жойланади ва сўнгра PPTP протоколи воситасида IP протоколининг пакетларига инкапсуляцияланади ва шу протокол ёрдамида шифрланган кўринишда ҳар қандай TCP/IP тармоғи орқали ташилади.

PPP сессияси доирасида узатилувчи пакетлар қуйидаги тузилмага эга (8.10-расм):

- Internet ичида ишлатилувчи канал сатҳининг сарлавхаси, масалан Ethernet кадрининг сарлавхаси;

- таркибида пакетни жўнатувчи ва қабул қилувчи адреслари бўлган IP сарлавҳаси;

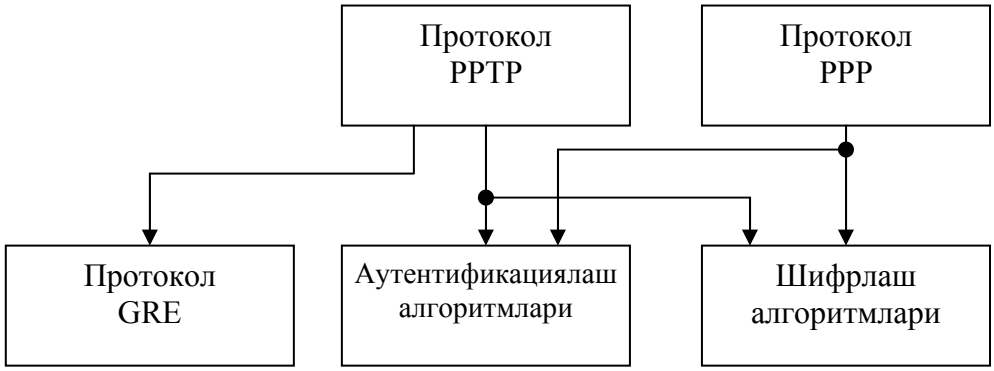
- маршрутлаш учун инкапсуляциялашнинг умумий усулининг сарлавҳаси GRE(Generic Routing Encapsulation);

- таркибида IP, IPX ёки NetBEUI пакетлари бўлган дастлабки пакет PPP.

8.10–расм. PPTP туннели бўйича жўнатилади пакет тузилмаси

Тармоқнинг қабул қилувчи узели IP пакетлардан PPP кадрларни чиқариб олади, сўнгра PPP кадрдан дастлабки пакет IP, IPX ёки NetBEUI пакетини чиқариб олиб уни локал тармоқ бўйича муайян адресатга жўнатади. Канал сатҳининг инкапсуляцияловчи протоколларининг кўп протоколлилиги (унга PPTP протокол ҳам тааллуқли), уларнинг янада юқорироқ сатҳнинг ҳимояланган канал протоколларидан афзаллигидир. Масалан, агар корпоратив тармоқда IPX ёки NetBEUI ишлатилса, IPSec ёки SSLпротоколларини ишлатиб бўлмайди, чунки улар IP тармоқ сатҳининг фақат битта протоколига мўлжалланган.

Инкапсуляциялашнинг мазкур усули OSI моделининг тармоқ сатҳи протоколларига боғлиқ бўлмасликни таъминлайди ва очиқ IP-тармоқлар орқали ҳар қандай локал тармоқлардан (IP, IPX ёки NetBEUI) ҳимояланган масофадан фойдаланишни амалга оширишга имкон беради. PPTP протоколига мувофиқ, ҳимояланган виртуал канал яратишда масофадаги фойдаланувчини аутентификациялаш ва узатилувчи маълумотларни шифрлаш амалга оширилади (8.11-расм).



8.11–расм. PPTP протоколи архитектураси

Масофадаги фойдаланувчини аутентификациялашда PPP учун қўлланиладиган турли протоколлардан фойдаланиш мумкин. Microsoft компанияси томонидан Windows 98/XP/NT/2000 га киритилган PPTPнинг амалга оширилишида аутентификациялашнинг қуйидаги протоколлари мададланади: парол бўйича аниқлаш протоколи PAP(Pasword Athentication Protocol), қўл беришишда аниқлаш протоколи MSCHAP (Microsoft Challenge – Handshaking Authentication Protocols) ва аниқлаш протоколи EAP-TLS (Extensible Authentication Protocol-Transport Layer Security). PAP про-

токолидан фойдаланилганда идентификаторлар ва пароллар алоқа линиялари орқали шифрланмаган кўринишда узатилади, бунда аутентификациялашни фақат сервер ўтказади. MSCHAP ва EAP-TLS протоколларидан фойдаланилганда нияти бузуқ одамнинг ушлаб қолинган шифрланган паролли пакетдан қайта фойдаланишидан ҳимоялаш ва мижоз ва VPN-серверни аутентификациялаш таъминланади.

PPTP ёрдамида шифрлаш Internet орқали жўнатишда маълумотлардан ҳеч ким фойдаланаолмаслигини кафолатлайди. Шифрлаш протоколи MPPE (Microsoft Point-to-Point Encryption) фақат MSCHAP(1 ва 2 версиялари) ва EAP-TLS билан бирга ишлайолади ва мижоз ва сервер орасида параметрлар мувофиқлаштирилишида шифрлаш калитининг узунлигини автоматик тарзда танлай олади. MPPE протоколи узунлиги 40, 56 ёки 128 бит бўлган калитлар билан ишлашни мададлайди.

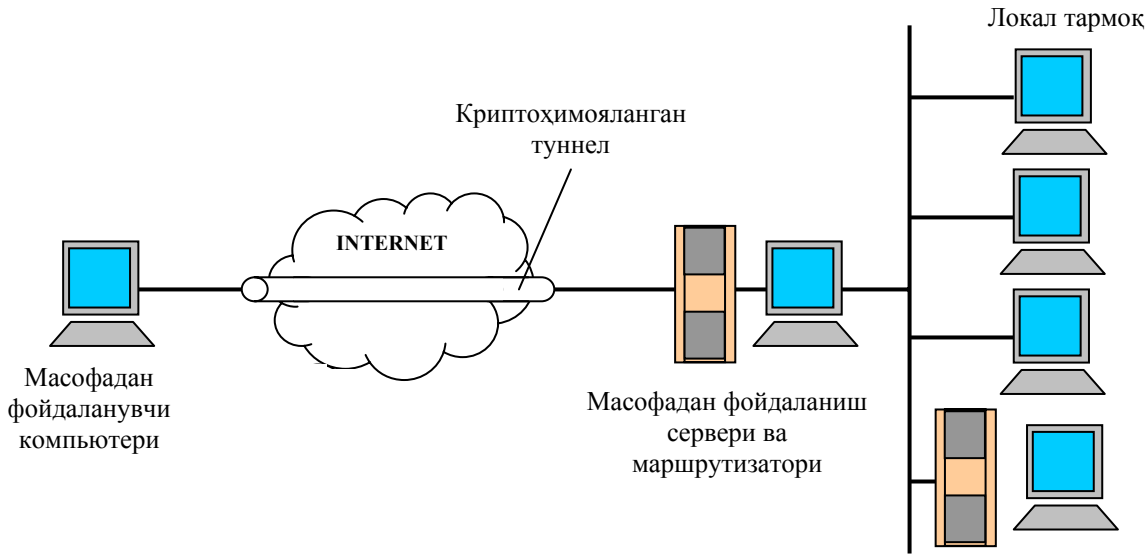
PPTP протоколи хар бир олинган пакетдан сўнг шифрлаш калити қийматини ўзгартиради. MMPE протоколи "нуқта-нуқта" хилидаги алоқа каналлари учун ишлаб чиқилган бўлиб, бу алоқа каналларида пакетлар кетма-кет узатилади ва малумотлар йўқотилиши жуда кам. Бу вазиятда навбатдаги пакет учун калит қиймати олдинги пакетнинг расшифровкаси натижасига боғлиқ. Умумфойдаланувчи тармоқ орқали виртуал тармоқ қуришда бу шартларга риоя қилиш мумкин эмас, чунки маълумотлар пакети кўпинча қабул қилувчига жўнатилган кетма-кетликда келмайди. Шунинг учун PPTP шифрлаш калитини ўзгартиришда пакетларнинг тартиб рақамидан фойдаланади. Бу расшифровка қилишни олдинги қабул қилинган пакетларга боғлиқ бўлмаган ҳолда амалга оширишга имкон беради.

PPTP протоколи учун қўллашнинг қуйидаги иккита асосий схемаси аниқланган:

- масофадан фойдаланувчининг Internet билан тўғридан-тўғри уланишидаги туннеллаш схемаси;

- масофадан фойдаланувчининг Internet билан провайдер орқали телефон линияси бўйича уланишидаги туннеллаш схемаси.

Туннеллашнинг биринчи схемаси амалга оширилганида (8.12-расм) масофадан фойдаланувчи Windows 98/XP/NT таркибидаги масофадан фой-

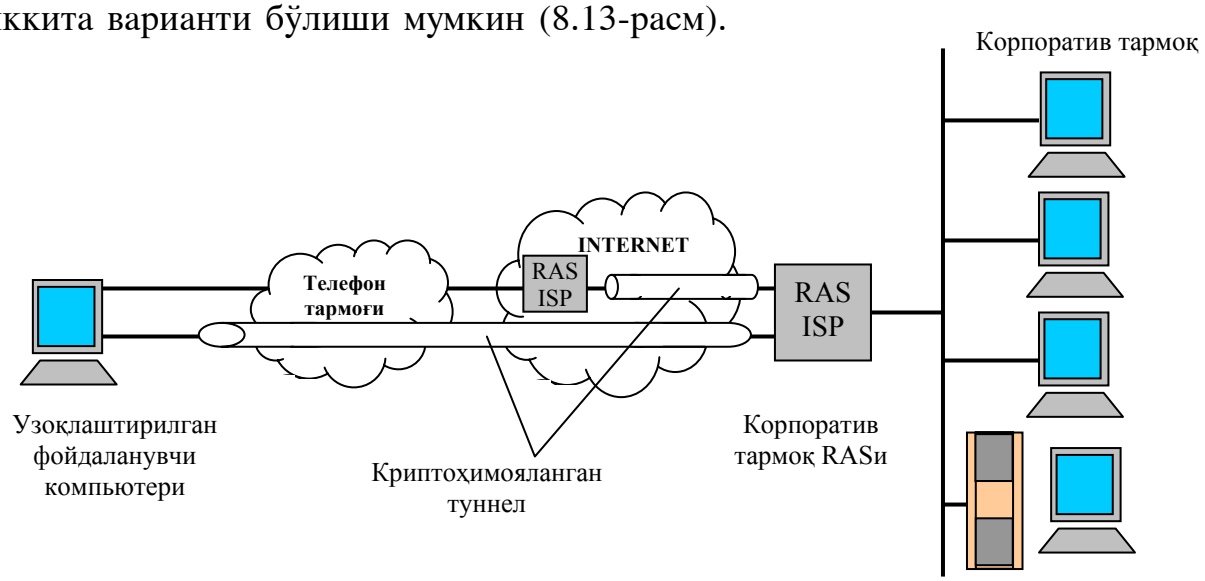


8.12 –расм. Масофадан фойдаланувчи компьютерини Internetга тўғридан-тўғри уланишидаги туннеллаш схемаси.

даланиш сервиси RAS (Remote Access Service)нинг мижоз қисми ёрдамида локал тармоқ билан масофавий боғланишни ўрнатади. Сўнгра фойдаланувчи локал тармоқдан масофадан фойдаланиш серверига, унинг IP адресини кўрсатиб мурожаат этади ва у билан PPTP протоколи бўйича алоқа ўрнатади.

Масофадан фойдаланиш сервери вазифасини локал тармоқнинг чегара маршрутизатори бажариши мумкин. Масофадан фойдаланувчининг компьютерида Windows 98/XP/NT таркибидаги RAS сервернинг мижоз қисми ва PPTPнинг драйвери, масофадан фойдаланувчи локал тармоғининг серверида эса Windows NT Server таркибидаги RAS сервери ва PPTP драйвери ўрнатилиши шарт. PPTP протоколи ўзаро алоқадаги томонлар алмашадиган бир нечта хизматчи хабарни аниқлайди. Хизматчи хабарлар TCP протоколи бўйича узатилади. Муваффақиятли аутентификациялашдан сўнг ҳимояланган алмашиш жараёни бошланади. Локал тармоқнинг ички серверлари PPTP протоколини мададламаслиги мумкин, чунки чегара маршрутизатор IP пакетлардан PPP кадрларини чиқариб олиб уларни локал тармоқ орқали керакли IP, IPX ёки NetBIOS форматида жўнатади.

Масофадаги компьютерни Internetга телефон линияси бўйича провайдер ISP (Internet Service Provider) орқали улашда туннеллаш схемасининг иккита варианти бўлиши мумкин (8.13-расм).



8.13–расм. Масофадан фойдаланувчи компьютерини ISP провайдери орқали телефон линиясидан фойдаланиб Internetга уланишини туннеллаш схемасининг иккита варианти.

Схеманинг биринчи вариантининг қурилиши протокол PPTPнинг провайдер ISPнинг масофадан фойдаланиш сервери ва чегара корпоратив маршрутизатор орқали мададланиши тахминига асосланган. Сервер одатда фойдаланувчиларнинг уланишини таъминловчи кўп сонли тезкорлиги паст портларга эга. Провайдер ISPнинг сервери RAS ва маршрутизатор орасида ҳимояланган канал ҳосил бўлади. Моҳияти бўйича бу – "шлюз-шлюз" хилидаги ҳимояланган канал варианти.

Бу вариантда масофадан фойдаланувчининг компьютери протокол PPTPни мададламаслиги мумкин. Масофадаги фойдаланувчи стандарт протокол PPP ёрдамида провайдер ISPда ўрнатилган масофадан фойдаланиш сервери RAS билан боғланади ва аутентификациялашни провайдерда ўтайди.

Провайдернинг сервери RAS фойдаланувчининг исми бўйича фойдаланувчиларнинг ҳисоб маълумотлари базасидан маршрутизаторнинг IP-адресини топади. Бу маршрутизатор чегара маршрутизатори ва ушбу фойдаланувчининг локал тармоқдан масофадан фойдаланиш сервери ҳисобланади. Бу маршрутизатор билан провайдер сервери RAS Intrenet орқали PPTP протоколи бўйича сессия ўтказади. Провайдернинг сервери

RAS локал тармоқдан масофадан фойдаланиш серверига фойдаланувчининг идентификаторини ва бошқа маълумотларни узатади. Улар асосида бу сервер CHAP протоколи бўйича фойдаланувчини яна аутентификациялайди. Агар фойдаланувчи иккинчи аутентификациялашдан (бу унинг учун шаффоф бўлади) муваффақиятли ўтса, провайдернинг RASи бу тўғрида фойдаланувчини PPP протокол бўйича огоҳлантиради ва сўнгра, провайдернинг масофадан фойдаланувчи сервери ва локал тармоқ орасида ҳимояланган виртуал канал шаклланади.

Масофадан фойдаланувчининг компьютери локал тармоқ IP, IPX, ёки NetBIOS билан ўзаро алоқа пакетларини PPP кадрларига жойлаб провайдернинг масофадан фойдаланувчи сервери RASга узатади. Провайдернинг RASи аталган адрес сифатида чегара маршрутизатори адресини, манба адреси сифатида ўзининг шахсий IP-адресини кўрсатган ҳолда PPP кадрларининг IP пакетларга инкапсуляциясини амалга оширади. Провайдернинг масофадан фойдаланувчи сервери ва локал тармоқ орасида узатишга аталган PPP пакетлари симметрик шифрда шифрланади. Бунда симметрик махфий калит сифатида CHAP протоколи бўйича аутентификациялаш учун провайдер RASининг ҳисоб маълумотларни базасида сақланувчи фойдаланувчи паролининг дайджести ишлатилади. Симметрик шифрлаш алгоритмлари сифатида DES ёки RC-4 алгоритм ишлатилади.

Тавсиф этилган вариант кенг тарқалмади, чунки протокол PPTP, асосан, Microsoft компаниясининг махсулотларида – RAS Windows NT 4.0 нинг мижоз ва сервер қисмларида, ҳамда RAS Windows 98/XPнинг мижоз қисмида амалга оширилган. Провайдерлар масофадан фойдаланиш сервери сифатида одатда RAS Windows NTга нисбатан қувватлироқ воситалардан фойдаланади. Бунда протокол PPTP Internet провайдерларининг масофадан фойдаланиш серверлари RAS орқали доимо мададланмайди. Ундан ташқари бу схемада маълумотлар фойдаланувчи компьютери ва Intrenet провайдери орасида ҳимояланмаган ҳолда узатилади, натижада унинг хавфсизлиги жиддий ёмонлашади.

Microsoft компанияси томонидан PPTP протоколини қўллашнинг яна бир бошқа схемаси таавсия этилган. Бу схемага биноан PPTP протоколи-

нинг провайдернинг масофадан фойдаланиш сервери томонидан мададланиши талаб этилмайди. Туннеллашнинг бу варианти (8.13-расм) кенг тарқалди.

Таъкидлаш лозимки, бу схемада корпоратив тармоқнинг чегара маршрутизатори, олдинги схемадагидек PPTP протоколни мададлаши шарт. Бундай маршрутизатор сифатида, хусусан, RAS хизмати ўрнатилган дастурий маршрутизатор Windows NT 4.0 ишлатилиши мумкин. Умуман, RAS хизмати ва PPTP протоколи ишлайдиган, масофадаги мижоз компьютер ива корпоратив тармоқ ичидаги компьютер орасида ҳимояланган канални яратиш мумкин.

Ушбу схемага биноан фойдаланувчи икки марта масофадан уланишни ўрнатиши лозим. Биринчи марта фойдаланувчи провайдернинг масофадан фойдаланиш серверига модем бўйича қўнғироқ қилиб, PPP протоколи бўйича у билан алоқа ўрнатади ва провайдер ISP томонидан мададланувчи протоколларнинг бирига (PAP ёки CHAP) ёки терминал диалогига мувофиқ аутентификациядан ўтади. ISP провайдерида аутентификациядан муваффақиятли ўтганидан сўнг фойдаланувчи локал тармоқдан масофадан фойдаланиш сервери билан, унинг IP-адресини кўрсатиб уланишни ўрнатади. Натижада масофадаги компьютер ва локал тармоқ RAS орасида PPTP протоколи бўйича сессия ўрнатилади. Мижоз яна, энди ўзининг корпоратив тармоғи серверида аутентификацияланади. Масофадан фойдаланиш сервери фойдаланувчининг ҳақиқийлигини ўзининг ҳисоб маълумотлари базаси асосида текширади. Муваффақиятли аутентификациялашдан сўнг ахборотни ҳимояланган алмашиш жараёни бошланади.

Криптоҳимояланган туннелнинг чегара қурилмаларининг ўзаро алоқаси учун PPTP протоколида бошқарувчи хабарлар кўзда тутилган бўлиб, бу бошқарувчи хабарлар туннелни ўрнатиш, мададлаш ва узиш учун аталган. Бошқарувчи хабарларни алмашиш мижоз ва PPTPнинг сервери орасида ўрнатилувчи TCP-уланиш бўйича амалга оширилади. Бу уланиш бўйича узатиладиган пакетларда канал сатҳи сарлавҳаси билан бир қаторда IP протоколининг сарлавҳаси, TCP протоколининг сарлавҳаси ва пакет маълумотлари соҳасидаги PPTPнинг бошқарувчи хабари бўлади.

L2F протоколи Cisco System компанияси томонидан OSI моделининг канал сатҳида ҳимояланган виртуал тармоқ қуриш учун, PPTP протоколига альтернатива сифатида ишлаб чиқилган. L2F протоколи турли тармоқ протоколлари томонидан мададланиши билан ажралиб туради ва Internet провайдерлари учун фойдаланишда анча қулай. L2F протоколи масофадаги фойдаланувчи компьютери билан провайдер сервери алоқасини ташкил этишда масофадан фойдаланишнинг турли протоколларини (PPP, SLIP ва ҳ.) ишлатишга йўл қуяди. Туннел орқали пакетларни ташишда ишлатилувчи очиқ тармоқ IP протоколи асосида ва бошқа, хусусан X.25 протоколи асосида ишлаши мумкин.

L2F протоколи қуйидаги хусусиятларга эга:

- ҳақиқийликни текширувчи муайян протоколга қатъий боғланмаганликни тахминловчи аутентификациялаш муолажаларининг мосланувчанлиги;

- охирги тизимлар учун шаффофлиги, яъни локаль тармоқнинг ишчи станциялари ва масофадаги тизимга ҳимоялаш серверидан фойдаланиш учун махсус дастурий таъминот талаб этилмайди;

- воситалар учун шаффофлиги, яъни масофадаги фойдаланувчиларни авторизациялаш локал тармоқнинг масофадан фойдаланиш серверига фойдаланувчиларни бевосита уланишига ўхшаб амалга оширилади;

- аудитнинг тўлиқлиги, яъни локал тармоқ серверидан фойдаланиш ходисасини қайдлаш нафақат масофадан фойдаланиш сервери тмонидан, балки провайдер сервери томонидан ҳам амалга оширилади.

L2F протоколининг спецификациясига мувофиқ ҳимояланган туннелни ҳосил қилишда қуйидаги протоколлар ишлатилади:

- дастлабки инкапсуляцияланувчи протокол - бу протокол (IP, IPX, ёки NetBEUI) асосида локал тармоқ ишлайди;

- протокол - "пассажир" – бу протоколга дастлабки протокол инкапсуляцияланади ва бу протоколнинг ўзи ҳам очиқ тармоқ орқали масофадан фойдаланганда инкапсуляцияланаши мумкин; PPP протоколи тавсия этилади;

- бошқарувчи (инкапсуляцияловчи) протокол, туннелни яратишда, мададлашда ва узишда ишлатилади (бундай протокол сифатида L2F ишлатилади);

- провайдер протоколи, инкапсуляцияланувчи протоколларни (даст-лабки протокол ва протокол – "пассажир") ташишда ишлатилади; энг кўп тарқалган провайдер протоколи IP протоколидир.

Таъкидлаш лозимки, L2F технологиясидан фойдаланилганда провайдернинг масофадан фойдаланиш сервери фойдаланувчини аутентификациялашни фақат виртуал канал яратилиши зарурлигини аниқлаш ва исталган локал тармоқнинг масофадан фойдаланиш сервери адресини топишда ишлатади. Ҳақиқийликни якуний текшириш локал тармоқнинг масофадан фойдаланиш сервери томонидан, у билан провайдер сервери уланганидан сўнг, бажарилади.

L2F протоколининг қуйидаги камчиликларини кўрсатиш мумкин:

- унда IP протоколининг жорий версияси учун ахборот алмашинувининг охирги нуқталари орасида криптоҳимояланган туннел яратиш кўзда тутилмаган;

- виртуал ҳимояланган канал фақат провайдернинг масофадан фойдаланиш сервери ва локал тармоқнинг чегара маршрутизатори орасида яратилиши мумкин, бунда масофадаги фойдаланувчи компьютери билан провайдер сервери орасидаги жой очиқ қолади.

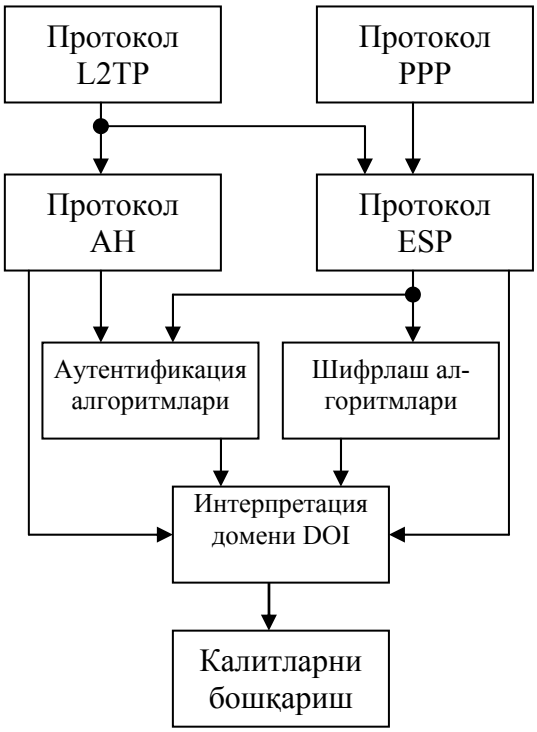
Ҳозирда L2F протоколи Internet стандарти лойиҳаси мақомига эга бўлган L2TP протоколига сингдирилган.

L2TP протоколи IETF ташкилотида Microsoft ва Cisco Systems компаниялари мададида ишлаб чиқилган. L2TP протоколи ихтиёрий муҳитли умуммақсад тармоқ орқали PPP-трафикни ҳимояланган туннеллаш протоколи сифатида ишлаб чиқилган.

PPTPдан фарқли ҳолда L2TP протоколи IP протоколига боғланган эмас, шу сабабали ундан пакетларни коммутацияловчи тармоқларда, масалан ATM (Asynchronous Transfer Mode) ёки кадрларни ретрансляцияловчи (frame relay) тармоқларда фойдаланиш мумкин.

L2TP протоколида PPTP ва L2F протоколларининг нафақат яхши хусусиятлари бирлаштирилган, балки янги функциялар, жумладан IPSec протоколлари стекининг AH ва ESP протоколлари билан ишлаш имконияти қўшилган.

L2TP протоколининг архитектураси 8.14–расмда келтирилган.



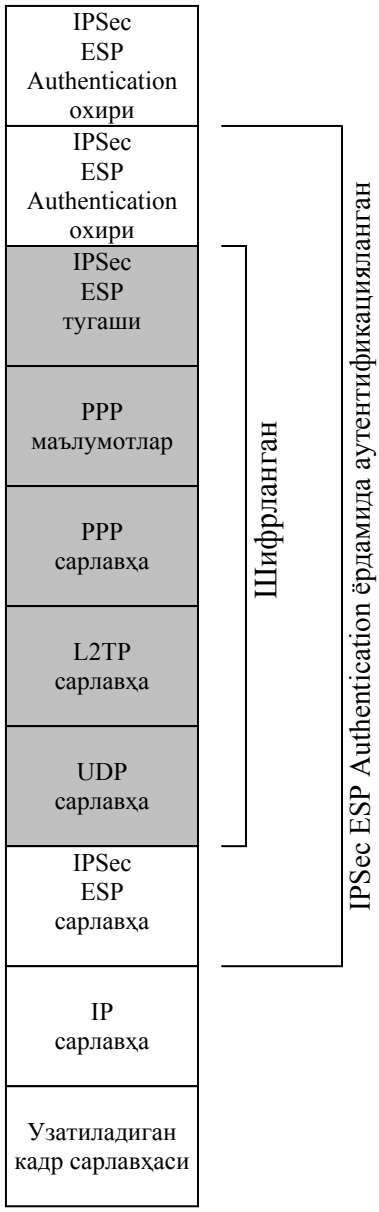
8.14 –расм. L2TP протоколининг архитектураси

AH ва ESP протоколлари фойдаланувчиларнинг, келишилган ҳолда, шифрлаш ва аутентификациялашнинг турли криптографик алгоритмларини ишлатишларига йўл қўяди. Интерпретация домени DOT (Domain of Interpretation) ишлатилувчи ва алгоритмларнинг бирга ишлашини таъминлаши бўйича, гибрид протокол L2TP масофадаги фойдаланувчиларни аутентификациялаш, ҳимояланган виртуал уланишни яратиш ва маълумотлар оқимларини бошқариш функциялари билан кенгайтирилган PPP протоколидир.

Майдони

L2TP протоколи транспорт сифатида UDP протоколини ишлатади ва туннелни бошқаришда ва маълумотларни ташишда хабарларнинг бир хил форматидан фойдаланади.

PPTP протоколидагидек, L2TP протоколи туннелга узатиш учун пакетни йиғишда аввал PPP ахборот маълумотлари майдонига PPP сарлавҳасини, сўнгра L2TP сарлавҳасини қўшади. Шу тариқа олинган пакет UDP протокол томонидан инкапсуляцияланади. L2TP протокол жўнатувчи ва қабул қилувчи порти сифатида UDP-портдан фойдаланади. 8.15–расмда L2TP туннели бўйича жўнатилувчи пакет тузилмаси келтирилган.



8.15–расм. L2TP туннели бўйлаб жўнатиладиган пакет тузилмаси

IPSec протоколлар стеки хавфсизлиги сиёсатининг танланган хилига боғлиқ ҳолда L2TP протоколи UDP-хабарни шифрлаши ва унга ESP (Encapsulation Security Payload)нинг сарлавхасини ва охирини ҳамда IPSec ESP Authenticationнинг охирини қўшиши мумкин. Сўнгра IPга инкапсуляциялаш бажарилади. Таркибида жўнатувчи ва қабул қилувчи адреслари бўлган IP-сарлавҳа қўшилади. Охирида L2TP маълумотларни узатишга тайёрлаш учун иккинчи PPP-инкапсуляциялашни бажаради.

Компьютер – қабул қилувчи маълумотларни қабул қилади. PPPнинг сарлавҳаси ва охирини ишлайди. IP сарлавҳани олиб ташлайди. IPSec ESP Authentication ёрдамида IP нинг ахборот майдони аутентификацияланади. IPSec ESP протоколи эса пакетнинг расшифровкасида ёрдам беради. Кейин компьтер UDP сарлавҳасини ишлайди ва туннелни идентификациялаш учун L2TP сарлавҳасидан фойдаланади. Энди PPP пакетнинг таркибида фақат фойдали маълумотлар бўлади, улар ишланади ва кўрсатилган қабул қилувчига юборилади.

L2TP протоколи "фойдаланувчи" ва "компьютер" сатҳларда аутентификациялашни таъминлайди, ҳамда маълумотларни аутентификациялайди ва

шифрлайди. Мижозларни ва VPN серверларини аутентификациялашнинг биринчи босқичида L2TP сертификация хизматидан олинган локал сертификатлардан фойдаланади. Мижоз ва сервер сертификатлар билан алмашишади ва ҳимояланган уланиш ESP SA (Security Association)ни яратишади.

L2TP компьютерни аутентификациялашни тугатганидан сўнг, фойдаланувчи сатҳда аутентификациялашда фойдаланувчи исмини ва паролни очиқ кўринишда узатувчи ҳар қандай протокол, ҳатто PAP, ишлатилиши мумкин. Бу тамомила хавфсиз, чунки L2TP бутун сессияни шифрлайди. Аммо фойдаланувчини аутентификациялашни, компьютер ва фойдаланувчини аутентификациялашда турли калитлардан фойдаланувчи MSCHAP ёрдамида ўтказиш хавфсизликни ошириш мумкин.

L2TP протоколининг тахмини бўйича провайдернинг масофадан фойдаланиш сервери ва корпоратив тармоқ маршрутизатори орасида туннел ҳосил қилувчи схемалардан фойдаланилади. Бу протокол олдингиларидан (PPTP ва L2F протоколларидан) фарқли ҳолда охирги абонентлар орасида, ҳар бири алоҳида иловага ажратилиши мумкин бўлган, бир неча туннелни бирданига очиш имкониятини тақдим этади. Бу хусусият туннеллашнинг мосланувчанлигини ва хавфсизлигини таъминлайди.

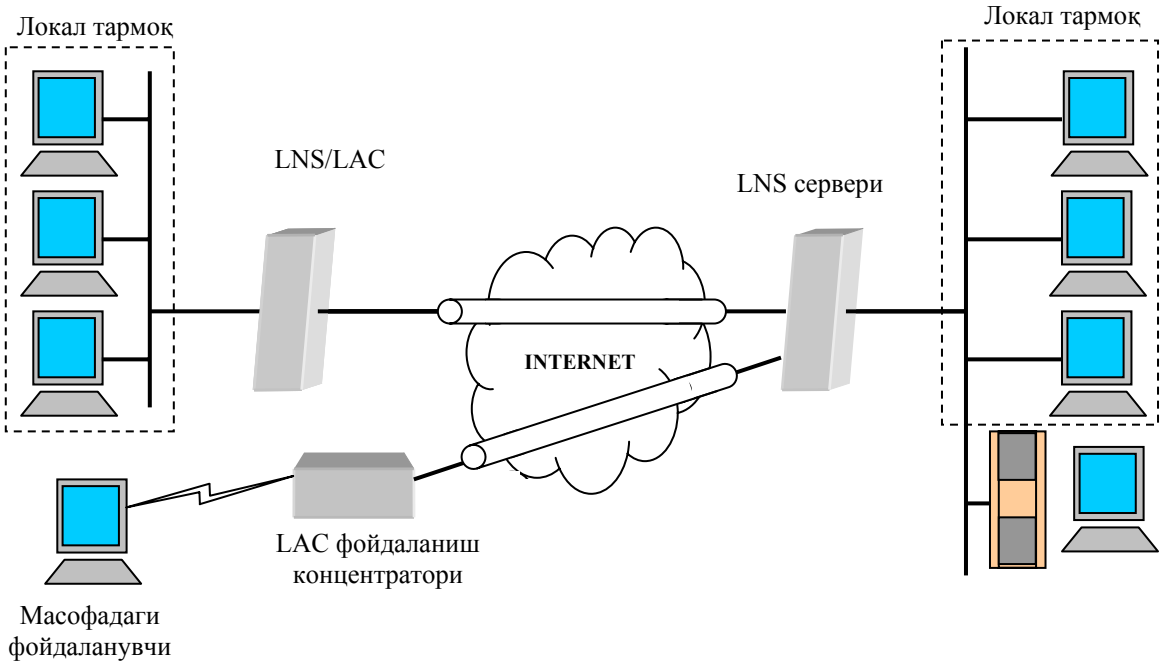
L2TP протоколининг спецификациясига биноан провайдернинг масофадан фойдаланиш сервери ролини, L2TP протоколининг мижоз қисмини амалга оширувчи ва масофадаги фойдаланувчига унинг локал тармоғидан Internet орқали тармоқли фойдаланишни таъминловчи, фойдаланишнинг концентратори LAC (L2TP Access Concentrator) бажариши лозим. Локал тармоқнинг масофадан фойдаланиш сервери сифатида PPP протоколи билан бирга ишлай олувчи платформаларда ишловчи тармоқ сервери LNS (L2TP Network Server)дан фойдаланилади (8.16-расм).

PPTP ва L2F протоколларидек L2TP протоколида ҳимояланган виртуал канални шакллантириш уч босқичда амалга оширилади:

- локал тармоқнинг масофадан фойдаланиш сервери билан уланишни ўрнатиш;

- фойдаланувчини аутентификациялаш;

- ҳимояланган туннелни конфигурациялаш.



8.16–расм. L2TP протоколи асосида туннеллаш схемаси.

Биринчи босқичда локал тармоқнинг масофадан фойдаланиш сервери билан уланишни ўрнатиш учун масофадаги фойдаланувчи провайдер ISP билан PPP – улашни бошлаб беради. Провайдер сервери ISPда ишловчи фойдаланиш концентратори бу уланишни қабул қилади ва канал PPPни ўрнатади. Сўнгра фойдаланувчи концентратори LAC охирги узел ва унинг фойдаланувчисини қисман аутентификациялайди. Провайдер ISP фақат фойдаланувчининг исмидан фойдаланган ҳолда унга L2TP туннеллаш сервисининг кераклигини ҳал қилади. Агар бундай сервис керак бўлса, фойдаланиш концентратори LAC туннели уланиш ўрнатилиши лозим бўлган тармоқ сервери LNS адресини аниқлашга ўтади. Фойдаланувчи ва фойдаланувчи тармоғига хизмат кўрсатувчи сервер LNS орасидаги мувофиқликни аниқлашнинг кулайлигини таъминлаш мақсадида провайдер ISP томонидан ўзининг мижозлари учун мададланувчи маълумотлар базасидан фойдаланиш мумкин.

LNS серверининг IP-адреси аниқланганидан сўнг L2TPнинг бу сервер билан туннели бор ёки йўқлиги текширилади. Агар бундай туннел бўлмаса, у ўрнатилади. Провайдернинг фойдаланиш концентратори LAC ва локал

тармоқнинг тармоқ сервери LNS орасида L2TP протокол бўйича сессия ўрнатилади.

Транспортга ўзаро алоқаннинг "нўқта-нуқта" пакет режимини мададалаши талаби қўйилади. LAC ва LNS орасида туннел яратишда бу туннел доирасида янги уланишга чақириш идентификатори Call ID деб аталувчи идентификатор берилади. Концентратор LAC тармоқ серверига ушбу Call ID билан чақириқ хусусидаги билдириш бўлган пакет жўнатади. LNS сервери чақириқни қабул қилиши ёки рад этиши мумкин.

Иккинчи босқичда локал тармоқнинг тармоқ сервери LNS фойдаланувчини аутентификациялаш жараёнини бажаради. Бунинг учун аутентификациялашнинг стандарт алгоритмларидан бири, хусусан CHAP алгоритми ишлатилиши мумкин. Таъкидлаш лозимки, L2TP протоколининг спецификациясида аутентификациялаш усулларининг тавсифи келтирилмаган. Чақириқ хусусидаги билдириш таркибида тармоқ сервери LNS томонидан фойдаланувчини аутентификациялаш учун ахборот бўлиши мумкин. Бу ахборотни концентратор LAC фойдаланувчи билан мулоқот жараёнида йиғади. Аутентификациялашнинг CHAP протоколидан фойдаланилганда билдириш пакетида чақириш-сўзи, фойдаланувчи исми ва унинг жавоби бўлади. PAP протоколи учун бу ахборот фойдаланувчи исми ва шифрланмаган паролдан иборат бўлади. Тармоқ сервери LNS бу ахборотдан, масофадаги фойдаланувчини ўз маълумотларини қайтадан киритишга мажбур қилмаслик ва аутентификациялашнинг қўшимча циклини бажармаслик мақсадида, бирданига фойдаланиш мумкин.

Аутентификация натижаси жўнатилишида тармоқ сервери LNS ҳам фойдаланиш концентратори LACга фойдаланувчи узелининг IP-адресини узатиши мумкин. Моҳияти бўйича фойдаланиш концентратори LAC масофадаги фойдаланувчи узели ва локал тармоқнинг тармоқ сервери орасида воситачи вазифасини бажаради. Масофадаги узелга корпоратив тармоқнинг адреслар пулидан адреснинг ажратилиши фойдаланувчига провайдер адреслар пулидан оддий адрес олинишидаги ноқулайликлардан кутилишига имкон беради.

Учинчи босқичда провайдернинг фойдаланиш концентратори LAC ва локал тармоқнинг сервери LNS орасида ҳимояланган туннел яратилади. Натижада инкапсуляцияланган кадрлар PPP туннел орқали концентратор LAC ва тармоқ сервери LNS орасида икала йўналишда узатилиши мумкин. Масофадаги фойдаланувчидан PPP кадри келганида концентратор LAC ундан кадрни қоплаган байтларни, назорат йиғинди байтларини чиқариб ташлайди, сўнгра уни L2TP протокол ёрдамида тармоқ протоколига инкапсуляциялайди ва туннел орқали тармоқ сервери LNSга жўнатади. LNS сервер L2TP протоколдан фойдаланиб, келган пакетдан PPP кадрни чиқариб олиб ишлайди.

Туннелнинг зарурий қийматларини созлаш бошқариш хабарлари ёрдамида амалга оширилади. L2TP протоколи ҳар қандай пакетни коммутацияловчи транспорт устидан ишлаши мумкин. Умумий ҳолда, бу транспорт, масалан UDP протоколи, пакетларни кафолатли етказиш ни таъминламайди. Шу сабабли L2TP протоколи бу масалаларни ҳар бир масофадаги фойдаланувчи учун туннел ичида уланишларни ўрнатиш муолажаларидан фойдаланиб, мустақил ҳал этади.

Таъкидлаш лозимки, L2TP протоколи криптоҳимоянинг муайян усулларини белгиламайди ва шифрлашни турли стандартларидан фойдаланиш мумкинлигини фараз қилади. Агар ҳимояланган туннелнинг IP-тармоқда шакллантирилиши режалаштирилган бўлса, криптоҳимояни амалга оширишда IPSec протоколидан фойдаланилади. L2TP протоколи PPP алгоритмига нисбатан маълумотларни ҳимоялашнинг юқори савиясини таъминлайди, чунки унда 3DES (Triple Data Encryption Standard) шифрлаш алгоритми ишлатилади. Агар ҳимоянинг бундан юқори савияси керак бўлмаса битта 56 хонали калитли DES алгоритмидан фойдаланиш мумкин. Ундан ташқари L2TP протоколи HMAC (Hash Massage Authentication Code) алгоритми ёрдамида маълумотларни аутентификациялашни таъминлайди. Аутентификациялаш учун бу алгоритм узунлиги 128 хонага тенг бўлган "хэш"ни яратади.

Шундай қилиб, PPTP ва L2TP протоколларининг функционал имкониятлари турлича, PPTP протоколи фақат IP-тармоқларда ишлатилиши

мумкин ва унга туннелни яратиши ва ишлатиши учун алоҳида TCP уланиш зарур. L2TP протоколи нафақат IP-тармоқларда ишлатилиши мумкин, туннелни яратиш ва у орқали маълумотларни ташишда хизматчи хабарлар бир хил формат ва протоколлардан фойдаланади. L2TP протоколи ташкилот учун муҳим бўлган маълумотларнинг қарийб 100%ли хавфсизлигини кафолатлаши мумкин.

L2TP протоколининг камчилиги сифатида қуйидагиларни кўрсатиш мумкин:

- L2TP протоколини амалга оширишда ISP провайдерларнинг мадади зарур;

- L2TP трафикни танланган туннел доирасида чегаралайди ва фойдаланувчиларнинг Internetнинг бошқа қисмларидан фойдаланишига имкон бермайди;

- L2TP протоколида IP протоколининг жорий версияси учун ахборот алмашинувнинг охирги нуқталари орасида криптоҳимояланган туннел яратиш кўзда тутилмаган;

- L2TPнинг таклиф этилган спецификацияси стандарт шифрлашни фақат IP-тармоқларда IPSec протоколи ёрдамида таъминлайди.

Сеанс сатҳида ҳимояланган виртуал каналларни шакллантириш протоколлари

Ҳимояланган виртуал каналларини шакллантириш мумкин бўлган OSI моделининг энг юқори сатҳи – бешинчи – сеанс сатҳидир. Сеанс сатҳида ҳимояланган виртуал тармоқни қуришда ахборот алмашинувини криптографик ҳимоялаш, жумладан, аутентификациялаш ҳамда ўзаро алоқа томонлари орасида воситачиликнинг қатор функцияларини амалга ошириш имконияти пайдо бўлади. Ҳақиқатан, OSI моделининг сеанс сатҳи мантиқий уланишларни ўрнатишга ва бу уланишларни бошқаришга жавобгар. Шу сабабли, бу сатҳда суралган уланишларнинг жоизлигини текширувчи ва тармоқлараро ҳаракатлар ҳимоясининг бошқа функцияларининг бажарилишини таъминлаовчи дастур-воситачилардан фойдаланиш имконияти мавжуд.

Сеанс сатҳида ҳимояланган виртуал канални шакллантириш протоколи ҳимоянинг татбиқий протоколлари ҳамда турли сервисларни тақдим

этувчи юқори сатҳ протоколлари (HTTP, FTP, POPS, SMTP ва ҳ. протоколлар) учун шаффофдир. Аммо, сеанс сатҳида юқори сатҳли протоколларни амалга оширувчи иловаларга бевосита боғлиқлик бошланади. Шунинг учун мазкур сатҳга мос келувчи ахборот алмашиш протоколини амалга ошириш кўп ҳолларда юқори сатҳли иловаларга ўзгартиришлар киритилишини талаб этади.

Сеанс сатҳида ахборот алмашишда SSL протоколи кенг тарқалган. Сеанс сатҳида ўзаро алоқа томонлари орасида воситачилик функцияларини бажариш учун IETF ташкилоти томонидан стандарт сифатида SOCKS протоколи қабул қилинган.

SSL протоколи Netscape Communication компанияси томонидан мижоз-сервер иловаларида ахборотни ҳимояланган алмашишни амалга ошириш учун ишлаб чиқилган. Ҳозирда SSL протоколи OSI моделининг сеанс сатҳида ишловчи ҳимояланган канал протоколи сифатида ишлатилади. Бу протокол ахборот алмашиш хавфсизлигини таъминлашда ахборотни ҳимоялашнинг криптографик усулларидан фойдаланади. SSLпротоколи тармоқнинг иккита абоненти орасида ҳимояланган канал қуришнинг барча функцияларини жумладан, уларни аутентификациялаш, узатилувчи маълумотларнинг конфиденциаллигини ва яхлитлигини таъминлаш функцияларини бажаради. Асимметрик ва симметрик криптотизимлардан комплекс фойдаланиш технологияси SSL протоколининг ядроси ҳисобланади.

SSLда иккала томоннинг ўзаро аутентификациялаш фойдаланувчиларнинг (мижоз ва сервер) махсус сертификация марказларининг рақамли имзоси билан тасдиқланган очиқ калитларининг рақамли сертификатлари билан алмашиш орқали бажарилади. SSL протоколи ҳамма қабул қилган X.509 стандартларга мос келувчи сертификатларни, ҳамда сертифкатларни беришда ва ҳақиқийлигини текширишда ишлатилувчи PKI очиқ калитлари инфратузилмаларининг стандартини мададлайди.

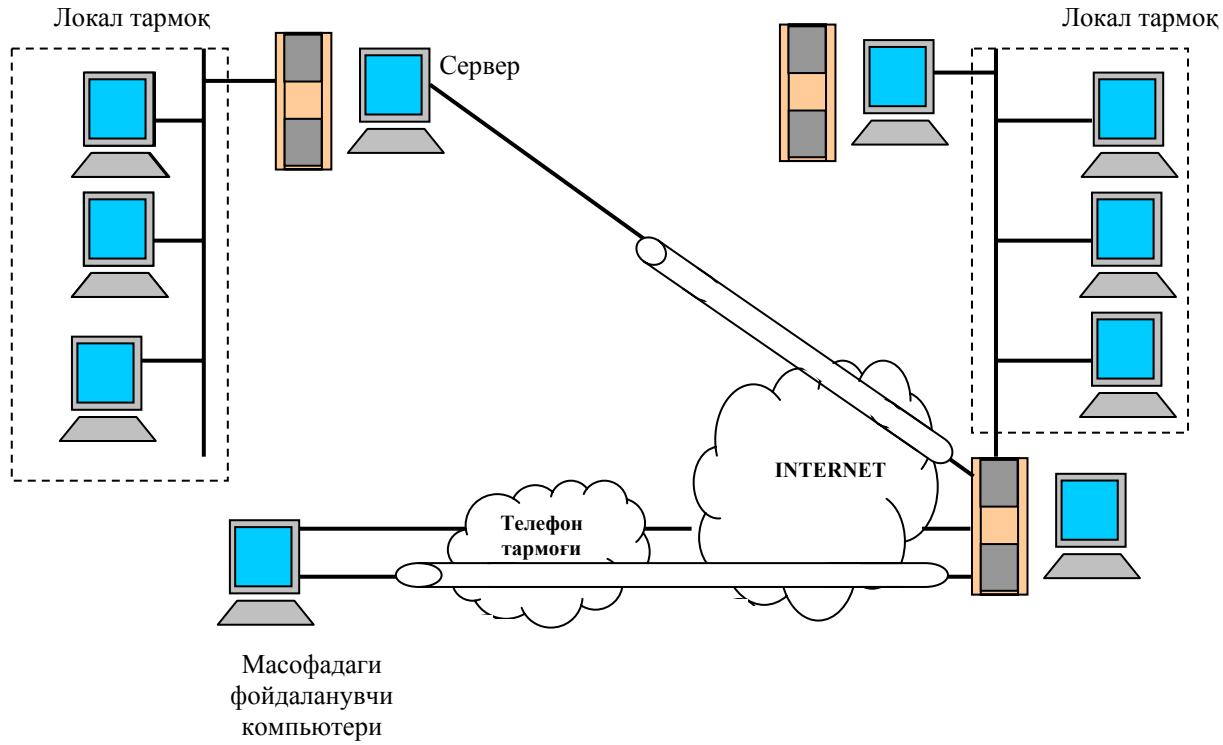
Конфиденциаллик уланиш ўрнатилишида томонлар алмашинадиган симметрик сессия калитларида узатилувчи хабарларни шифрлаш орқали таъминланади. Сессия калитлари ҳам шифрланган кўринишда узатилади. Бунда улар абонентларнинг сертификатларидан чиқариб олинган очиқ ка-

литларда шифрланади. Ахборотларни шифрлашда симметрик калитларнинг ишлатилишига асосий сабаб-симметрик калитларда шифрлаш ва расшифровка қилиш жараёнининг тезлиги асимметрик калитлар ишлатилишидагига қараганда юқорилиги.

Айланувчи ахборотнинг ҳақиқийлиги ва яхлитлиги электрон рақамли имзони шакллантириш ва текшириш эвазига таъминланади.

Асимметрик шифрлаш алгоритмлари сифатида RSA, ҳамда Диффи-Хеллман алгоритмлари ишлатилади. Симметрик шифрлаш алгоритмлари сифатида эса RC2, RC4, DES ҳамда Triple DES алгоритмлари ишлатилади. Хэш функцияларини ҳисоблашда MD5 ва SHA-1 стандартлари ишлатилиши мумкин. SSL протоколининг 3.0 версиясида криптографик алгоритмлари тўплами кенгайтирилувчи ҳисобланади.

SSL протоколига мувофиқ криптоҳимояланган туннеллар виртуал тармоқнинг охирги нуқталари орасида яратилади. Ҳар бир ҳимояланган туннелни бошлаб берувчилари-туннел охирги нуқталаридаги компьютерларда ишловчи мижоз ва сервер (8.17-расм).



8.17–расм. SSL протоколи асосида шаклланган криптоҳимояланган туннеллар.

Ҳимояланган уланишни шакллантиришда ва мададлашда SSL протоколи мижоз ва сервер ўзаро алоқасининг қуйидаги босқичларини кўзда тутади:

- SSL сессиясини ўрнатиш;
- ҳимояланган ўзаро алоқа.

SSL сессияни ўрнатиш жараёнида қуйидаги масалалар ечилади:

- томонларни аутентификациялаш;
- ҳимояланган ахборот алмашинувида ишлатилувчи криптографик алгоритмлар ва зичлаштириш алгоритмларини мувофиқлаштириш;
- умумий маҳфий мастер-калитни шакллантириш;
- ахборот алмашишни криптографик ҳимоялаш учун шакллантирилган мастер-калит асосида умумий маҳфий сеанс калитларини генерациялаш.

Қўл беришиш муолажаси деб ҳам аталувчи SSL-сессияни ўрнатиш муолажаси ахборот алмашишни бевосита ҳимоялашдан олдин пухта ишланади ва SSL протоколи таркибига кирувчи бошланғич саломлаш (Hand-Shake Protocol) протоколи бўйича бажарилади.

Мижоз ва сервер орасида қайта уланиш ўрнатилишида томонлар, ўзаро келишув бўйича, олдинги умумий сир асосида янги сеанс калитларини шакллантиришлари мумкин (ушбу муолажа SSL-сессиянинг давоми деб аталади).

SSL 3.0 протоколи аутентификациялашнинг қуйидаги учта режимини мададлайди:

- томонларни ўзаро аутентификациялаш;
- мижозни аутентификацияламасдан серверни бир томонлама аутентификациялаш;
- тўлиқ анонимлик.

Охирги вариантдан фойдаланилганда томонларнинг ҳақиқийлигини кафолатламасдан ахборот алмашиш хавфсизлиги таъминланади. Бу ҳолда ўзаро алоқадаги томонлар, алоқа қатнашчиларини алмаштириб қўйиш билан боғлиқ хужумлардан ҳимояланмайдилар.

SSL протоколига мувофиқ ўзаро алоқадаги томонларни аутентификациялашда ва умумий махфий калитни шакллантиришда кўпинча RSA алгоритмидан фойдаланилади.

Очиқ калитлар ва уларнинг эгалари орасидаги мувофиқлик махсус сертификация марказлари томонидан берилувчи рақамли сертификатлар ёрдамида ўрнатилади. Сертификат таркибида қуйидаги ахборот бўлган маълумотлар блокидир:

- сертификация марказининг номи;
- сертификат эгасининг исми;
- сертификат эгасининг очиқ калити;
- сертификатнинг таъсир муддати;
- идентификатор ва сертификатни ишлашда фойдаланиладиган криптоалгоритмнинг параметрлари;
- сертификат таркибидаги барча маълумотларни тасдиқловчи сертификация марказининг рақамли имзоси.

Сертификат таркибидаги сертификация марказининг рақамли имзоси очиқ калит ва унинг эгасининг ҳақиқийлигини ва бир маънода мослигини таъминлайди. Сертификация маркази очиқ калитларнинг ҳақиқийлигини тасдиқловчи нотариус ролини утайди. Натижада бу калит эгаларига ҳимояланган ўзаро алоқа хизматидан, олдиндан шахсий учрашувсиз фойдаланишларига имкон беради.

1999 йили SSL 3.0версияси ўрнига, SSL протоколига асосланган ва ҳозирда Internet стандарти ҳисобланган TLS протоколи келди. SSL 3.0 ва TLS протоколлари орасидаги фарқ жуда ҳам жиддий эмас.

SSL ва TLS протоколларининг камчилиги - ўзларининг хабарларини ташишда тармоқ сатҳидаги фақат битта – IP-протоколидан фойдаланишлари ва, демак, фақат IP-тармоқларда ишлайолишлари. Ундан ташқари, SSL/TLSнинг амалда қўлланиши татбиқий протоколлар учун тўла шаффоф эмас.

SSLнинг яна бир салбий томони шундай иборатки, агар мижоз ва сервер уланишни узсалар, улар уни маълумотларнинг минимал ҳажмини алмашиш йўли билан тиклашлари ва Session ID нинг эски параметрларидан

фойдаланишлари мумкин. Нияти бузуқ одам олдинги сессиялардан бирини обрўсизлантириб уни тиклаш муолажасини сервер билан ўтказиши мумкин. Натижада бу сессияда узатиладиган кейинги барча маълумотлар обрўсизлантирилади.

Ундан ташқари, SSLда аутентификациялашда ва ширфлашда бир хил калитдан фойдаланилади. Бу эса маълум бир ҳолатларда заифликка олиб келиши мумкин. Бундай ечим турли калитлар ишлатилганига нисбатан кўп статистик маълумотларни йиғишга имкон беради.

SOCKS протокли OSI моделининг сеанс сатҳида мижоз-сервер иловаларининг ўзаро алоқа муолажасини сервер-воситачи ёки proxy-сервер орқали ташкил этади.

Умумий ҳолда, тармоқлараро экранларда анъанавий ишлатилувчи дастур-воситачилар қуйидаги функцияларни бажариши мумкин:

- фойдаланувчини идентификациялаш ва аутентификациялаш;
- узатилувчи маълумотларни криптоҳимоялаш;
- ички тармоқ ресурсларидан фойдаланишни чегаралаш;
- ахборотлар оқимини фильтрлаш ва ўзгартириш, масалан, вирусларни қидириш ва ахборотни шаффоф шифрлаш;
- чиқадиган ахборот оқимлари учун ички тармоқ адресларини трансляциялаш.

Аввал SOCKS протоколи фақат мижоз иловаларининг серверга сўровларини қайта йўналтириш, ҳамда бу иловаларга олинган жавобни қайтариш учун ишлаб чиқилган эди. Ушбу муолажаларнинг ўзи тармоқ IP-адреслари NATни (Network Address Translation) трансляциялаш функцияларини амалга ошириш имкониятини беради. Чиқувчи пакетлардаги жўнатувчиларнинг IP-адресларини шлюзининг битта IP-адреси билан алмаштириш ички тармоқ топологиясини ташқи фойдаланувчилардан беркитишга имкон беради ва натижада, рухсатсиз фойдаланиш масаласи мураккаблашади. Тармоқ адресларини трансляциялаш хавфсизликни ошириш билан бир қаторда хусусий адреслаш тизимини мададлаш имконияти ҳисобига тармоқ ички адреси маконини кенгайтиришга имкон беради.

SOCKS протоколи асосида тармоқли ўзаро алоқани ҳимоялаш бўйича воситачиликнинг бошқа функциялари ҳам амалга оширилиши мумкин. Масалан, SOCKS ахборот оқимлари йўналишни назоратлашда ва фойдаланувчилар ва ахборотлар атрибутларига боғлиқ ҳолда фойдаланишни чегаралашда ишлатилиши мумкин. SOCKS протоколининг воситачилик функцияларини бажаришдаги самарали ишлатилиши унинг OSI моделининг сеанс сатҳига мўлжалланганлиги билан таъминланади. Татбиқий сатҳдаги воситачиларга қараганда, сеанс сатҳида энг юқори тезкорликка, юқори сатҳ протоколларига (HTTP, FTP, POPS, SMTP ва ҳ.) боғлиқ бўлмасликка эришилади. Ундан ташқари SOCKS протоколи IP протоколга боғланмаган ва операцион тизимга боғлиқ эмас. Масалан, мижоз иловалари ва воситачи орасида ахборот алмашишда IPX протоколи ишлатилиши мумкин.

SOCKS протоколи туфайли тармоқлараро экранлар ва виртуал хусусий тармоқлар турли тармоқлар орасида хавфсиз ўзаро алоқани ва ахборот алмашинувини ташкил этишлари мумкин. SOCKS протоколи ушбу тизимларни хавфсиз бошқаришни унификацияланган стратегия асосида амалга оширишга имкон беради. Таъкидлаш лозимки, SOCKS протоколи асосида ҳар бир илова ва ҳар бир сеанс учун алоҳида ҳимояланган туннел яратилиши мумкин.

SOCKS протоколи спецификациясига мувофиқ тармоқ шлюзига (тармоқлараро экранга) ўрнатилувчи SOCKS – *сервер* ва ҳар бир фойдаланувчи компьютерга ўрнатилувчи SOCKS – *мижоз* фарқланади. SOCKS-сервер ҳар қандай татбиқий сервер билан бу серверга мос келувчи татбиқий мижоз номидан ўзаро алоқани таъминлайди. SOCKS-мижоз мижоз томонидан татбиқий серверга бўлган барча сўровларни ушлаб қолиб уларни SOCKS-сервер узатишга аталган. Таъкидлаш лозимки, мижоз иловаларининг сўровларини ва SOCKS-сервер билан ўзаро алоқани ушлаб қолишни бажарувчи SOCKS-мижозлар универсал мижоз дастурларига ўрнатилиши мумкин. SOCKS-серверга сеанс (сокет) сатҳидаги трафик маълум, шунинг учун у синчиклаб назоратлаши, хусусан, фойдаланувчиларнинг муайян иловалари ишини, агар уларнинг ахборот алмашишга зарур ваколатлари бўлмаса, блокировка қилиши мумкин. SOCKS протоколининг 4- ва 5- вер-

сиялари кенг тарқалган. Ҳозирда SOCKS протоколининг 5-версияси IETF ташкилоти томонидан Internetнинг стандарти сифатида маъқулланган.

SOCKS протоколининг 4-версиясига биноан уланишни ўрнатишнинг умумий схемаси қуйидагича:

- тармоқдаги қандайдир сервер билан боғланишни истаган мижоз SOCKS-сервер (ихтисослаштирилган proxy-сервер) билан уланиб унга махсус сўров юборади. Бу сўровда IP-адрес ва у уланиши керак бўлган масофадаги сервер порти бўлади;

- SOCKS-сервер масофадаги сервер-адресат билан уланади;

- мижоз ва масофадаги сервер уланиш занжири бўйича ўзаро алоқа қилади, SOCKS-сервер маълумотларни ретрансляциялайди;

SOCKS протоколининг 5-версияси тўртинчи версиянинг жиддий ривожи ҳисобланади. У қуйидаги қўшимча имкониятларни амалга оширади:

- номларидан SOCKS-мижозлар мурожаат этувчи фойдаланувчиларни аутентификациялаш кўзда тутилган. SOCKS-сервер SOCKS-мижоз билан аутентификациялаш усулини келишиб олишлари мумкин. Аутентификациялаш компьютер ресурсларидан фойдаланишни чегаралашга имкон беради. Икки томонлама аутентификациялаш ҳам жоиз ҳисобланади, яъни фойдаланувчи, ўз навбатида, керакли SOCKS-сервер билан уланганига ишонч ҳосил қилиши мумкин;

- доменли исмларни ишлатиш жоиз ҳисобланади: SOCKS-мижоз SOCKS-серверга нафақат уланишни ўрнатишда керак бўлган компьютернинг IP-адресини, балки унинг DNS исмини ҳам узатиши мумкин;

- нафақат TCP-протокол, балки UDP протокол ҳам мададланади;

SOCKS протоколининг 5-версиясига биноан уланишни ўрнатишнинг умумий схемаси қуйидагича тавсифланиши мумкин:

- тармоқдаги қандайдир татбиқий сервер билан уланиш ўрнатишни истаган татбиқий мижознинг сўровини мана шу компьютерда ўрнатилган SOCKS-мижоз ушлаб қолади;

- SOCKS-сервер билан уланган SOCKS-мижоз унга ўзи мададловчи аутентификациялашнинг барча усулларининг идентификаторларини билдиради;

- SOCKS-сервер аутентификациялашнинг қайси усулидан фойдаланишни ҳал қилади (агар SOCKS-сервер SOCKS-мижоз томонидан таклиф этилган аутентификациялаш усулларидан бирортасини ҳам мададламаса, уланиш узилади);

- таклиф этилган аутентификациялаш усулидан бирортаси мададланса SOCKS сервер танланган усул бўйича фойдаланувчини (унинг номидан SOCKS-мижоз қатнашади) аутентификациялайди; муваффақиятсиз аутентификациялашда SOCKS-сервер уланишни узади;

- муваффақиятли идентификациялашдан кейин SOCKS-мижоз SOCKS-серверга тармоқдаги сўралаётган татбиқий сервер DNS исмини ёки IP-адресини узатади, сўнгра SOCKS-сервер фойдаланишни чегаралашнинг мавжуд қоидалари асосида ушбу татбиқий сервер билан уланишни ўрнатиш бўйича қарор қабул қилади;

- уланиш ўрнатилган ҳолда татбиқий мижоз ва татбиқий сервер бир-бирлари билан уланиш занжири орқали алоқа қиладилар; SOCKS-сервер маълумотларни ретрансляциялайди, ҳамда тармоқли ўзаро алоқа хавфсизлиги бўйича воситачилик функцияларини бажариши мумкин; масалан, аутентификациялаш жараёнида SOCKS-мижоз ва SOCKS-сервер сеанс калитларини алмаштиришган бўлсалар, улар орасидаги барча трафик шифрланиши мумкин.

Фойдаланувчиларни SOCKS-сервер томонидан аутентификациялаш X.509 форматидаги рақамли сертификатларга ёки паролларга асосланиши мумкин. SOCKS-мижоз ва SOCKS-сервер орасидаги трафикни шифрлаш учун OSI моделининг сеансли ёки пастроқ сатҳларига мўлжалланган протоколлар ишлатилиши мумкин. SOCKS-сервер фойдаланувчиларни аутентификациялаш, IP-адресларини трансляциялаш ва трафикни криптоҳимоялашдан бошқа яна қуйидаги функцияларни бажариши мумкин:

- ички тармоқ ресурсларидан фойдаланишни чегаралаш;

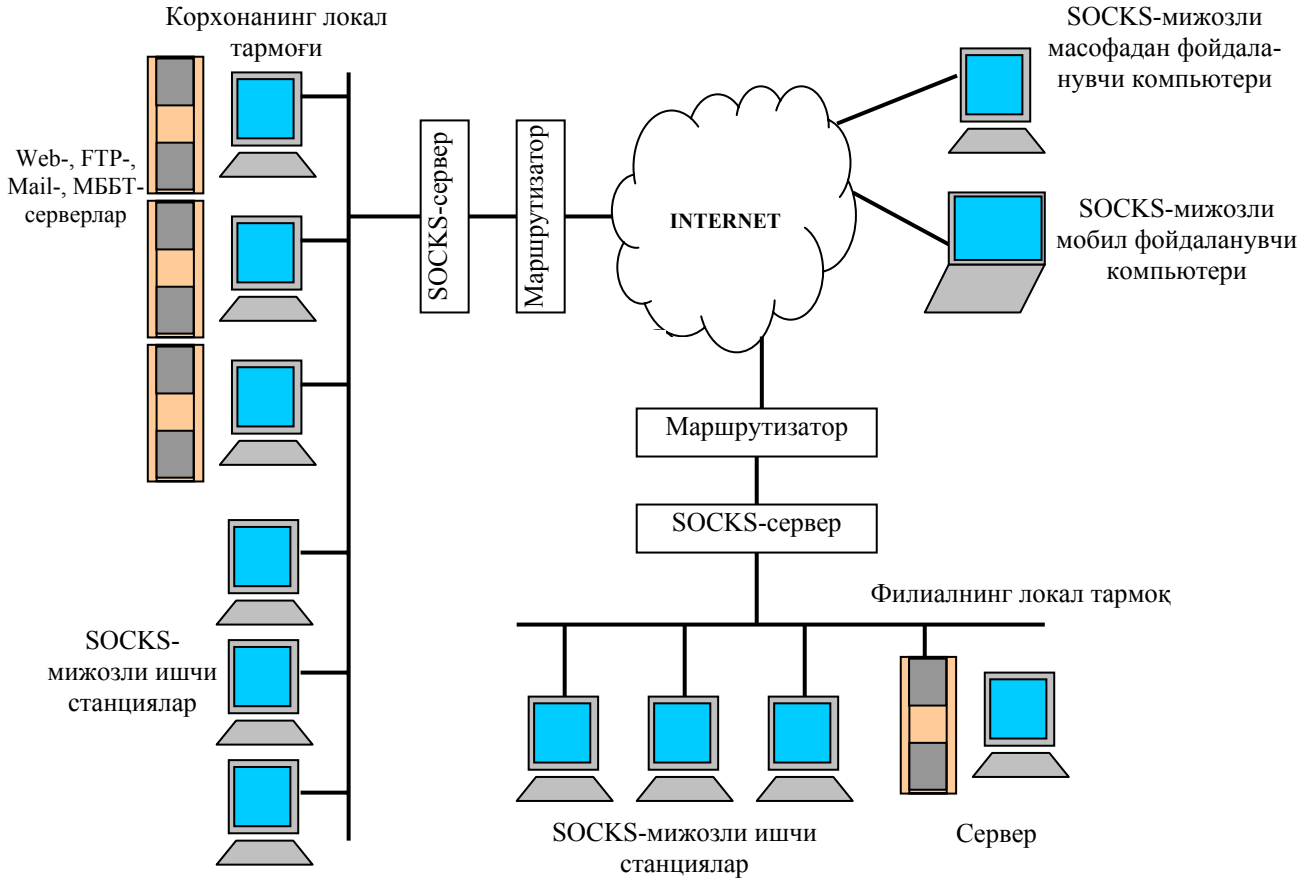
- ташқи тармоқ ресурсларидан фойдаланишни чегаралаш;

-хабарлар оқимини фильтрлаш, масалан вирусларни динамик қидириш;

- ходисаларни қайдлаш ва уларга реакция кўрсатиш;

- ташқи тармоқдан сўралган маълумотларни кэшлаш.

Шундай қилиб, SOCKS протоколи бўйича ҳимояланган виртуал тармоқларни шакллантириш учун ҳар бир локал тармоқ билан Internet уланган нуқтадаги компьютер-шлюзда SOCKS-сервер, локал тармоқдаги ишчи станцияларда ва масофадан фойдаланувчиларнинг компьютерларида эса SOCKS-мижоз ўрнатилади. Моҳияти бўйича, SOCKS-серверга SOCKS протоколини мададловчи тармоқлараро экран сифатида қараш мумкин (8.18-расм).



8.18–расм. SOCKS протоколи бўйича ўзаро алоқа схемаси.

Масофадаги фойдаланувчилар Internetга коммутацияланувчи ёки ажратилган линиялар орқали уланишлари мумкин. Ҳимояланган виртуал тармоқ фойдаланувчиси қандайдир татбиқий сервер билан уланишга уринганида SOCKS-мижоз SOCKS-сервер билан ўзаро алоқани бошлайди. Ўзаро алоқанинг биринчи босқичи тугаганидан сўнг фойдаланувчи аутентификацияланади, фойдаланиш қоидаси эса унинг кўрсатилган адресдаги компью-

терда ишлайдиган муайян тармоқ иловаларига уланиш ҳуқуқига эга эканлигини кўрсатади. Кейинги ўзаро алоқалар криптографик ҳимояланган канал бўйича юз бериши мумкин.

SOCKS-серверга, локал тармоқларни рухсатсиз фойдаланишдан ҳимоялашдан ташқари, бу локал тармоқ фойдаланувчиларининг Internetнинг очиқ ресурсларидан (Telnet, WWW, SMTP, POP ва ҳ.) фойдаланишларининг назорати ҳам юкланиши мумкин. Фойдаланиш бутунлай авторизацияланган, чунки фойдаланувчининг компьютери эмас, балки ўзи идентификацияланади ва аутентификацияланади. Фойдаланиш қоидалар муайян ходимнинг ваколатига кўра Internetнинг маълум ресурслари билан боғланишга рухсат бериши ёки бермаслиги мумкин. Фойдаланиш қоидаларининг таъсири бошқа параметрлар, масалан, аутентификациялаш усули ёки сутка вақтига боғлиқ бўлиши мумкин. Тармоқли ўзаро алоқа хавфсизлигининг янада юқори даражасига эришиш учун Internet томонидан фойдаланишга рухсат берилган локал тармоқ серверлари, SOCKS-серверга уланувчи, ҳимояланган очиқ қисм тармоқни ҳосил қилувчи алоҳида сегментга ажратилишлаш лозим.

8.5. IPSec протоколлар стекини ҳимояланган виртуал хусусий тармоқлар қуришда ишлатилиши

IPSec протоколи (Internet Protocol Security) асосан IP тармоқларда маълумотларни хавфсиз узатишни таъминлашга аталган. IPSecнинг ишлатилиши қуйидагиларни кафолатлайди:

- узатилаётган маълумотларнинг яхлитлигини, яъни маълумотлар узатилишида бузилмайди, йўқолмайди ва такрорланмайди;

- жўнатувчининг аутентлигини, яъни маълумотлар ҳақиқий жўнатувчи томонидан узатилган;

- узатиладиган маълумотларнинг конфиденциаллигини, яъни маълумотлар шундай шаклда узатиладики, уларни рухсатсиз кўздан кечиришнинг олди олинади.

Таъкидлаш лозимки, маълумотлар хавфсизлиги тушунчасига одатда, яна бир талаб-маълумотларнинг фойдаланувчанлиги киритилади. Маълумотларнинг фойдаланувчанлиги деганда маълумотлар етказилишининг кафолати тушунилади. IPSec протоколлари бу масалани ҳал этмайди ва уни транспорт сатҳи ISPга қолдиради. IPSec протоколлар стеки тармоқ сатҳида ахборот ҳимоясини таъминлайди. Бу ҳимоянинг ишловчи иловаларга кўринмаслигига олиб келади.

IP-пакет IP тармоқларда коммуникациянинг фундаментал бирлиги ҳисобланади. Унинг тузилмаси 8.19-расмда келтирилган. IP-пакет таркибида манба адреси S ва ахборот қабул қилувчининги адреси D, транспорт сарлавҳаси, бу пакетда ташилувчи маълумотлар хили хусусидаги ахборот ва маълумотларнинг ўзи бўлади.

8.19–расм. IP-пакет тузилмаси

Аутентификациялашни, узатилувчи маълумотларнинг конфиденциаллиги ва яхлитлигини таъминлаш мақсадида, IPSec протоколларининг стеки қатор стандартлаштирилган криптографик технологиялар асосида қурилган:

- калитларни алмаштириш очиқ тармоқдан фойдаланувчилар орасида махфий калитларни тақсимлашнинг Диффи-Хеллман алгоритми бўйича амалга оширилади;

- иккала томоннинг ҳақиқийлигини кафолатлаш ва main-in-the-midle хилидаги хужумларни олдини олиш мақсадида Диффи-Хеллман алгоритми бўйича алмашишларни имзолашда очиқ калитлар криптографиясидан фойдаланилади;

- очиқ калитларнинг ҳақиқийлигини тасдиқлашда рақамли сертификатлар ишлатилади;

- маълумотларни шифрлашда блокли симметрик алгоритмлардан фойдаланилади;

- хэшлаш функциялари асосида ахборотларни аутентификациялаш алгоритмлари ишлатилади.

Ҳимояланган канални ўрнатиш ва мададлашдаги асосий масалалар қуйидагилар:

- фойдаланувчилар ёки компьютерларни аутентификациялаш;

- ҳимояланган каналнинг охирги нуқталари орасида узатилувчи маълумотларни шифрлаш ва аутентификациялаш;

- каналнинг охирги нуқталарини маълумотларни аутентификациялашда ва шифрлашда керак бўладиган махфий калитлар билан таъминлаш.

Юқорида санаб ўтилган масалаларни ҳал этишда IPSec тизими ахборот алмашиш хавфсизлиги воситаларининг комплексидан фойдаланади.

IPSec протоколининг аксарият амалга оширилишида қуйидаги компонентлардан фойдаланилади:

- IPSecнинг асосий протоколи. Ушбу компонент ҳимояни инкапсуляцияловчи протокол ESP (Encapsulation Security Payload)ни ва сарлавҳани аутентификацияловчи протоколи AH(Authentication Header)ни амалга оширади. У сарлавҳаларни ишлайди; пакетга қўлланиладиган хавфсизлик сиёсатини аниқлаш учун SPD ва SAD маълумотлар базаси билан ўзаро алоқа қилади;

- калит ахборотларини алмашишни бошқариш протоколи IKE. IKE одатда фойдаланиш сатҳида қўлланилади (операцион тизимга ўрнатилгани бундан истисно);

- хавфсизлик сиёсатларининг маълумотлар базаси SPD (Security Policy Database). Бу энг муҳим компонентлардан бири бўлиб, пакетга қўлланиладиган хавфсизлик сиёсатини белгилайди. SPD дан асосий протокол IPSec томонидан кирувчи ва чиқувчи пакетларни ишлашда фойдаланилади;

- хавфсиз ассоциацияларнинг маълумотлар базаси SPD (Security Association Database). Бу маълумотлар базаси кирувчи ва чиқувчи ахборотни ишлаш учун хавфсиз ассоциациялар SA(Security Association) рўйхатини сақлайди. Чиқувчи SAлардан чиқувчи пакетларни ҳимоялашда, кирувчи SAлардан эса IPSec сарлавҳали пакетларни ишлашда фойдаланилади. SAD маълумотлар базаси SA билан қўлда ёки калитларин бошқариш протоколлари IKE ёрдамида тўлдирилади;

- хавфсизлик сиёсатини ва хавфсиз ассоцияцияларни бошқариш. Бу – хавфсизлик сиёсатини ва SAни бошқарувчи иловалар.

Асосий протокол IPSec (ESP ва AHни амалга оширувчи) TCP/IP протоколларининг транспорт ва тармоқ стеклари билан ўзаро узвий алоқада бўлади. IPSecни тармоқ сатҳининг қисми дейиш мумкин. IPSecнинг асосий модули иккита интерфейсни – кириш йўли ва чиқиш йўли интерфейсларни таъминлайди. Кириш йўли интерфейси кирувчи пакетлар томонидан, чиқиш йўли интерфейси эса чиқувчи пакетлар томонидан фойдаланилади. IPSecнинг амалга оширилиши TCP/IP протоколлар стекининг транспорт ва тармоқ сатҳлари орасидаги интерфейсга боғлиқ бўлмаслиги лозим.

SPD ва SAD маълумотлар базаси IPSec ишлашига жиддий таъсир кўрсатади. Улардаги маълумотлар тузилмасини танлаш IPsec ишлашининг унумдорлигига таъсир этади.

IPSecдаги барча протоколларни иккита гуруҳга ажратиш мумкин:

- узатилувчи маълумотларни бевосита ишловчи (уларнинг хавфсизлигини таъминлаш учун) протоколлар;

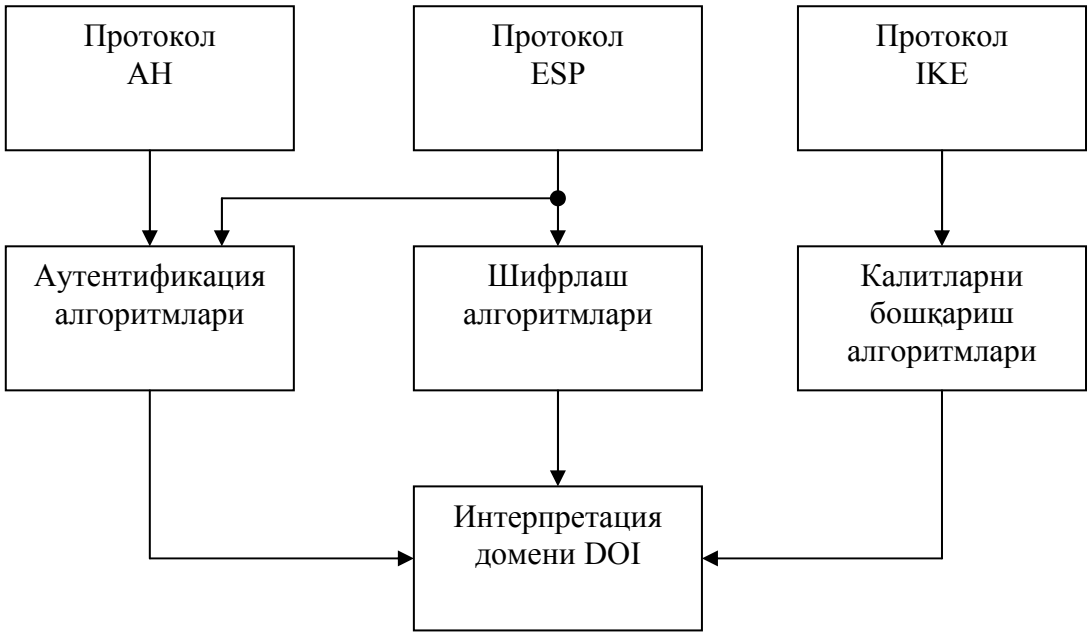
- биринчи гуруҳ протоколларига керакли ҳимояланган уланишлар параметрларини автоматик тарзда мувофиқлаштиришга имкон берувчи протоколлар.

IPSec ядросини учта AH, ESP ва виртуал канал ва калитларни бошқариш IKE параметрларини мувофиқлаштирувчи протоколлар ташкил этади.

IPSecнинг хавфсизлик воситаларининг архитектураси 8.20-расмда келтирилган.

Архитектуранинг *юқори сатҳида* қуйидаги протоколлар жойлашган:

- виртуал канал параметрларини мувофиқлаштирувчи ва калитларни бошқариш протоколи IKE. Бу протокол ҳимояланган канални инициализациялаш усулини, жумладан ишлатилувчи криптоҳимоялаш алгоритмларини мувофиқлаштиришни ҳамда ҳимояланган уланиш доирасида махфий калитларни алмашиш ва бошқариш муолажаларини белгилайди;



8.20–расм. IPSec протоколлари стекининг архитектураси

- сарлавҳани аутентификацияловчи протокол AH. Бу протокол маълумотлар манбаини аутентификациялашни, уларнинг, қабул қилинганидан сўнг, яхлитлигини ва ҳақиқийлигини текшириш ва такрорий ахборотларнинг тиқиштирилишидан ҳимояни таъминлайди;

- ҳимояни инкапсуляцияловчи протокол ESP. Бу протокол узатилувчи маълумотларни криптографик беркитишни, аутентификациялашни ва яхлитлигини таъминлайди ҳамда такрорий ахборотларнинг тиқиштирилишидан ҳимоялайди.

AH ва ESP протоколлари ҳар бири алоҳида ва биргаликда ишлатилиши мумкин. Бу протоколлар вазифаларининг қисқача баёнидан кўриниб турибдиики, уларнинг имкониятлари қисман бир хил.

AH протоколи фақат маълумотларни яхлитлигини ва аутентификациялашни таъминлашга жавоб беради. ESP протоколи қувватлироқ ҳисобланади, чунки у маълумотларни шифрлаши мумкин, ундан ташқари AH протоколи вазифасини ҳам бажариши мумкин.

IKE, AH ва ESP протоколларининг ўзаро алоқалари қуйидагича кечади. Аввал IKE протоколи бўйича иккита нуқта орасида мантиқий уланиш ўрнатилади. Бу уланиш IPSec стандартларида "хавфсиз ассоциация"-Security Association, SA номини олган. Ушбу мантиқий канал ўрнатилишида канал-

нинг охирги нуқталарини аутентификациялаш бажарилади ҳамда маълумотларни ҳимоялаш параметрлари, масалан, шифрлаш алгоритми, сессия махфий калити ва ҳ. танланади. Сўнгра хавфсиз ассоциация SA томонидан ўрнатилган доирада АНва ESP протоколи ишлай бошлайди. Бу протоколлар ёрдамида узатилувчи маълумотларнинг исталган ҳимояси, танланган параметрлардан фойдаланилган ҳолда, бажарилади.

IPSec архитектурасининг *ўрта сатҳини* IKE протоколида қўлланилувчи параметрларни мувофиқлаштириш ва калитларни бошқариш алгоритмлари ҳамда АН ва ESP протоколларида ишлатилувчи аутентификациялаш ва шифрлаш алгоритмлари ташкил этади.

Таъкидлаш лозимки, IPSec архитектурасининг юқори сатҳидаги виртуал канални ҳимоялаш протоколлари (АН ва ESP) муайян криптографик алгоритмларга боғлиқ эмас. Аутентификациялаш ва шифрлашнинг кўп сонли турли-туман алгоритмларидан фойдаланиш имконияти туфайли IPSec тармоқни ҳимоялашни ташкил этишнинг юқори даражада мосланувчанлиги таъминлайди. IPSecнинг мосланувчанлиги деганда ҳар бир масала учун унинг ечилишининг турли усуллари тавсия этилиши тушунилади. Бир масала учун танланган усул, одатда, бошқа масалаларни амалга ошириш усулларига боғлиқ эмас. Масалан, шифрлаш учун DES алгоритмининг танланиши маълумотларни аутентификациялашда ишлатилувчи дайджестни ҳисоблаш функциясини танлашга таъсир қилмайди.

IPSec архитектурасининг *пастки сатҳи* интерпретациялаш домени DOI (Domain of Interpretation)дан иборат. Интерпретациялаш доменининг қўлланиш заруриятига қуйидагилар сабаб бўлди. АН ва ESP протоколлари модулли тузилмага эга, яъни фойдаланувчилар ўзаро келишилган ҳолда шифрлаш ва аутентификациялашнинг турли криптографик алгоритмларидан фойдаланишлари мумкин. Шу сабабли, барча ишлатилувчи ва янги киритилувчи протокол ва алгоритмларнинг биргаликда ишлашини таъминловчи модул зарур. Айнан шу вазифалар интерпретациялаш доменига юклатилган.

Интерпретациялаш домени маълумотлар базаси сифатида IPSecда ишлатиладиган протоколлар ва алгоритмлар, уларнинг параметрлари, протокол идентификаторлари ва ҳ. хусусидаги ахборотларни сақлайди. Моҳияти

бўйича интерпретациялаш домени IPSec архитектурасида фундамент ролини бажаради. AH ва ESP протоколларида аутентификациялаш ва шифрлаш алгоритмлари сифатида миллий стандартларга мос келувчи алгоритмлардан фойдаланиш учун бу алгоритмларни интерпретациялаш доменида руйхатдан ўтказиш лозим.

AH ёки ESP протоколлари узатилувчи маълумотларни қуйидаги иккита режимда ҳимоялаши мумкин:

- туннел режимда; IP пакетлар бутунлай, уларнинг сарлавҳаси билан бирга ҳимояланади.

- траспорт режимида; IP пакетларнинг фақат ичидагилари ҳимояланади.

Туннел режими асосий режим ҳисобланади. Бу режимда дастлабки пакет янги IP пакетга жойланади ва маълумотлар тармоқ бўйича узатиш янги IP-пакет сарлавҳаси асосида амалга оширилади. Туннел режимида ишлашда ҳар бир оддий IP-пакет криптоҳимояланган кўринишда бутунлайча IPSec конвертига жойланади. IPSec конверти, ўз навбатида бошқа ҳимояланган IP-пакетга инкапсуляцияланади. Туннел режими одатда махсус ажратилган хавфсизлик шлюзларида - маршрутизаторлар ёки тармоқлараро экранларда амалга оширилади. Бундай шлюзлар орасида ҳимояланган туннеллар шакллантирилади.

Туннелнинг бошқа томонида қабул қилинган ҳимояланган IP-пакетлар "очилади" ва олинган дастлабки IP-пакетлар қабул қилувчи локал тармоқ компьютерларига стандарт қоидалар бўйича узатилади. IP-пакетларни туннеллаш туннелларни эгаси бўлмиш локал тармоқдаги оддий компьютерлар учун шаффоф ҳисобланади. Охирги тизимларда туннел режими масофадаги ва мобил фойдаланувчиларни мададлаш учун ишлатилиши мумкин. бу ҳолда фойдаланувчилар компьютерида IPSecнинг туннел режимини амалга оширувчи дастурий таъминот ўрнатилиши лозим.

Транспорт режимида тармоқ орқали IP-пакетни узатиш бу пакетнинг дастлабки сарлавҳаси ёрдамида амалга оширилади. IPSec конвертига криптоҳимояланган кўринишда фақат IP-пакет ичидаги жойланади ва олинган конвертга дастлабки IP-сарлавҳа қўшилади. Транспорт режими туннел

режимига нисбатан тезкор ва охирги тизимларда қўлланиш учун ишлаб чиқилган. Ушбу режим масофадаги ва мобил фойдаланувчиларни ҳамда локал тармоқ ичидаги ахборот оқимини ҳимоялашни мададлашда ишлатилиши мумкин. Таъкидлаш лозимки, транспорт режимида ишлаш ҳимояланган ўзаро алоқа гуруҳига кирувчи барча тизимларда ўз аксини топади ва аксарият ҳолларда тармоқ иловаларини қайта дастурлаш талаб этилади.

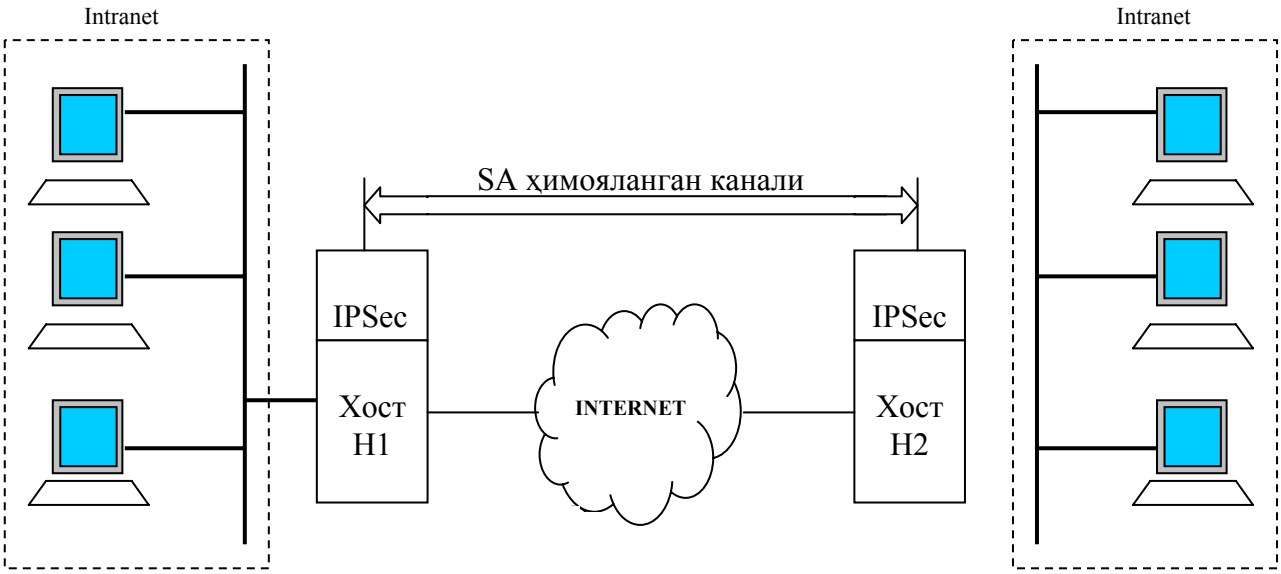
Туннел ёки транспорт режимидан фойдаланиш маълумотларни ҳимоялашга қуйиладиган талабларга ҳамда IPSec ишловчи узел ролига боғлиқ. Ҳимояланувчи канални тугалловчи узел-хост(охирги узел) ёки шлюз (ораликдаги узел) бўлиши мумкин. Мос ҳолда, IPSecни қўллашнинг қуйидагиучта асосий схемаси фарқланади:

- "хост - хост";
- "шлюз – шлюз";
- "хост - шлюз";

Биринчи схемада ҳимояланган канал тармоқнинг охирги иккита узели, яъни H1 ва H2 хостлар орасида ўрнатилади (8.21-расм), IPSecни мададловчи хостлар учун транспорт, ҳам туннел режимларидан фойдаланишга рухсат берилади.

8.21 расм. "Хост-хост" схемаси

Иккинчи схемага биноан, ҳимояланган канал ҳар бирида IPSec протоколи ишловчи, *хавфсизлик шлюзлари SG1 ва SG2* (Security Gateway) деб аталувчи ораликдаги иккита узеллар орасида ўрнатилади (8.22-расм).

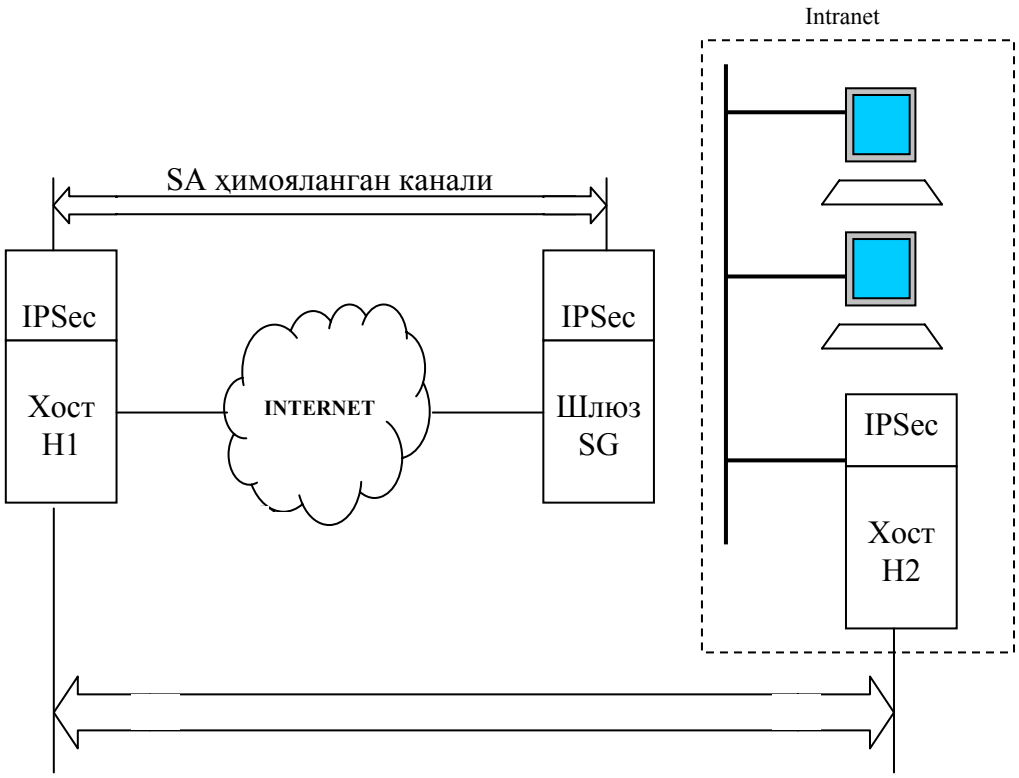


8.22-расм. "Шлюз-шлюз" схемаси

Хавфсизлик шлюзи иккита тармоққа уланувчи тармоқ қурилмаси бўлиб, ўзидан кейин жойлашган хостлар учун шифрлаш ва аутентификациялаш функцияларини бажаради. VPNнинг хавфсизлик шлюзи алоҳида дастурий маҳсулот, алоҳида аппарат қурилма ҳамда VPN функциялари билан тўлдирилган маршрутизатор ёки тармоқлараро экран кўринишида амалга оширилиши мумкин.

Маълумотларни ҳимояланган алмашиш тармоқларга уланган, хавфсизлик шлюзларидан кейин жойлашган ҳар қандай иккита охирги узеллар орасида руй бериши мумкин. Охирги узеллардан IPSec протоколни мададлаш талаб қилинмайди, улар ўзларининг трафигини ҳимояланмаган ҳолда корхонанинг ишончли тармоғи Intranet орқали узатади. Умумфойдаланувчи тармоққа юборилувчи трафик хавфсизлик шлюзи орқали ўтади ва бу шлюз ўзининг номидан IPSec ёрдамида трафикни ҳимоялашни таъминлайди. Шлюзларга фақат туннел режимида ишлашга рухсат берилади, гарчи улар транспорт режимини ҳам мададлашлари мумкин (бу ҳолда самара кам бўлади).

"Хост - шлюз" схемаси кўпинча ҳимояланган масофадан фойдаланишда ишлатилади (8.23-расм).



8.23-расм. "Хост-хост" канали билан тўлдирилган "хост-шлюз" схемаси

Бу ерда ҳимояланган канал IPSec ишловчи масофадаги H1 хост ва корхона Intranet тармоғига кирувчи барча хостлар учун трафикни ҳимояловчи SG шлюз орасида ташкил этилади. Масофадаги хост шлюзга пакетларни жўнатишда ҳам транспорт ва ҳам туннел режимларидан фойдаланиши мумкин, шлюз эса хостга пакетларни фақат туннел режимида жўнатади.

Бу схемани масофадаги H1 хост ва шлюз томонидан ҳимояланувчи ички тармоққа тегишли бирор H2 хост орасида параллел яна бир ҳимояланган каналнн яратиб модификациялаш мумкин. Иккита SAдан бундай комбинациялаб фойдаланиш ички тармоқдаги трафикни ҳам ишончли ҳимоялашга имкон беради.

Кўрилган IPSec асосида ҳимояланган каналнн қуриш схемалари турли-туман виртуал ҳимояланган тармоқларни (VPN) яратишда кенг қўлланилади. IPSec асосида турли архитектурага эга бўлган виртуал ҳимояланган тармоқлар, жумладан масофадан фойдаланувчи VPN(Remote Access VPN), корпорация ичидаги VPN(Intranet VPN) ва корпорацияларо VPN(Extranet VPN) қурилади.

IPSec асосидаги VPN-технологияларининг жозибалилигини қуйидаги сабаблар орқали изоҳлаш мумкин:

- тармоқ сатҳининг ҳимояси тармоқда ишловчи барча татбиқий тизимлар учун шаффоф, яъни барча иловалар ҳимояланган тармоқда ҳеч қандай тузатишсиз ва ўзгаришсиз худди очиқ тармоқда ишлаганидек ишлайверади;

- ҳимоялаш тизимининг масштабланувчанлиги таъминланади, яъни мураккаблиги ва унумдорлиги турли бўлган объектларни ҳимоялаш учун мураккаблиги, унумдорлиги, нархи даражаси бўйича адэкват бўлган ҳимоялашнинг дастурий ёки дастурий-аппарат воситаларидан фойдаланиш мумкин;

- масштабланувчи қатордаги ахборотни ҳимоялаш маҳсулотлари бирга ишлай оладилар, шу сабабли уларни турли сатҳдаги объектларда (масофадаги ягона терминаллардан то ихтиёрий масштабли локал тармоқларгача) ресурсларидан ва трафигидан барча бегоналар фойдаланаоломайдиган ягона корпоратив тармоққа бирлаштириш мумкин.

IX боб. ОЧИҚ КАЛИТЛАРНИ БОШҚАРИШ ИНФРАТУЗИЛМАСИ PKI

9.1. PKIнинг ишлаш принципи

Тарихан ахборот хавфсизлигини бошқарувчи ҳар қандай марказнинг вазифалари доирасига ахборот хавфсизлигининг турли воситалари томонидан ишлатилувчи калитларни бошқариш кирган. Бу-калитларни бериш, янгилаш, бекор қилиш ва тарқатиш.

Симметрик криптографиядан фойдаланилганда калитларни тарқатиш масаласи энг мураккаб муаммога айланган, чунки:

- N фойдаланувчи учун ҳимояланган N(N-1)/2 калитни тарқатиш лозим эди. N бир неча юзга тенг бўлганида бу сермашаққат вазифага айланиши мумкин;

- бундай тизимнинг мураккаблиги (калитларнинг кўплиги ва тарқатиш каналининг махфийлиги) хавфсизлик тизимини қуриш қоидаларининг биритизим оддийлигига тўғри келмайди, натижада заиф жойларнинг пайдо бўлишига олиб келади.

Асимметрик криптография фақат N махфий калитни тавсия этиб, бу муаммони четлаб ўтишга имкон яратади. Бунда ҳар бир фойдаланувчида фақат битта махфий калит ва махсус алгоритм бўйича махфий калитдан олинган очиқ калит бўлади.

Очиқ калитдан маҳфий калитни олиб бўлмаслиги сабабли очиқ калитни ҳимояланмаган ҳолда барча ўзаро алоқа қатнашчиларига тарқатиш мумкин. Ўзининг маҳфий калити ва ўзаро алоқадаги шеригининг очиқ калити ёрдамида ҳар қандай фойдаланувчи ҳар қандай криптоамалларни бажариши мумкин: бўлинувчи сирни ҳисоблаш, ахборотнинг конфиденциаллиги ва яхлитлигини ҳимоялаш, электрон рақамли имзони яратиш.

Шундай қилиб, симметрик криптографиянинг иккита асосий муаммоси ҳал этилади:

- калитлар сонининг кўплиги – улар энди атиги Nта;

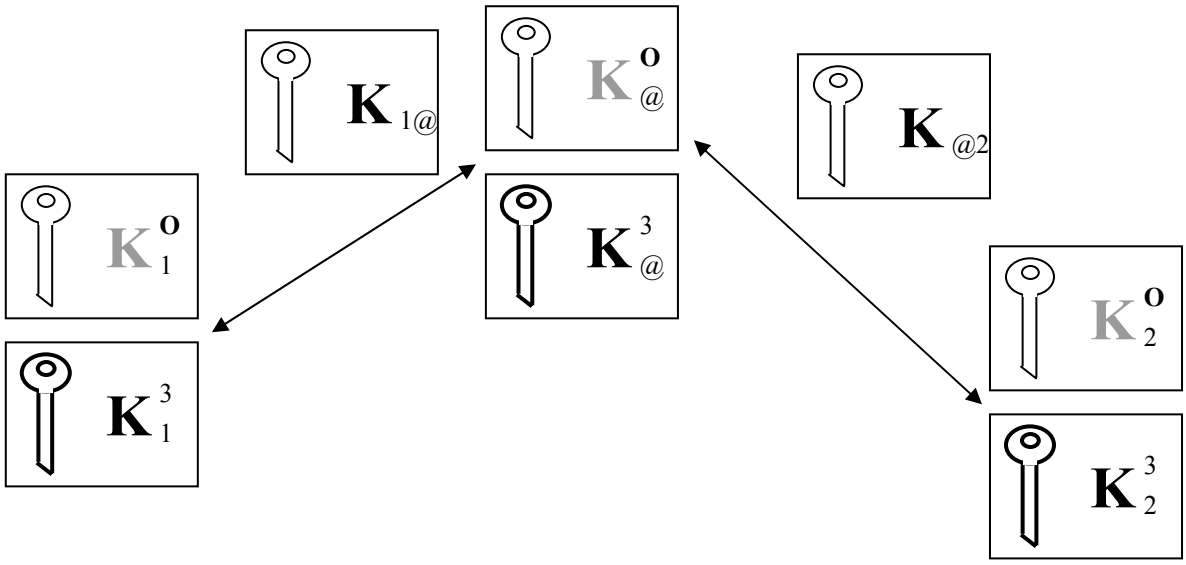
- тарқатишнинг мураккаблиги – уларни очиқ тарқатиш мумкин.

Аммо бу технологиянинг битта камчилиги – хужум қилувчи нияти бузуқ одам ўзаро алоқа қатнашчилари ўртасида жойлашганида man-in-the-middle (ўртадаги одам) хужумига мойиллиги.

Очиқ калитларни бошқариш инфратузилмаси PKI ушбу камчиликни бартараф қилишга имкон беради ва man-in-the-middle хужумидан самарали ҳимояланишни таъминлайди. Очиқ калитлар инфратузилмаси корпоратив ахборот тизимларининг ишончли ишлаши учун аталган ва ички ва ташқи фойдаланувчиларга ишончли муносабатлар занжири ёрдамида хавфсиз ахборот алмашишга имкон беради. Очиқ калитлар инфратузилмаси фойдаланувчининг шахсий махфий калитини унинг очиқ калити билан боғловчи электрон паспортга ўхшаб ишловчи рақамли сертификатларга асосланади.

Man-in-the-middle хужумидан ҳимоялаш. Man-in-the-middle хужуми амалга оширилганида нияти бузуқ одам очиқ канал орқали узатилувчи ўзаро алоқанинг қонуний иштирокчилари калитларини секингина ўзининг очиқ калитига алмаштириб, қонуний иштирокчиларнинг ҳар бири билан бўлинувчи сир яратиши ва сўнгра уларнинг барча ахборотларини ушлаб қолиши ва расшифровка қилиши мумкин.

Хужум қилувчининг ҳаракатини ва бу хужумдан ҳимояланиш усулини мисол орқали (9.1-расм) кўриб чиқайлик. Фараз қилайлик, фойдаланувчилар 1 ва 2 ўзларига умумий бўлган бўлинувчи сирни Диффи-Хеллман схемаси бўйича ҳисоблаб, ҳимояланган уланишни ўрнатишга қарор қилдилар. Аммо 1- ва 2- фойдаланувчиларнинг K_1 ва K_2 калитлари узатилаётган онда нияти бузуқ, одам @ адресатга етказмай ушлаб қолди. Нияти бузуқ одам ўзининг махфий ва очиқ калитини яратиб, очиқ K калитини 1 ва 2-фойдаланувчиларга секингина уларнинг ҳақиқий очиқ K_1 ва K_2 калитларининг ўрнига жўнатади. Натижада 1 ва 2 – фойдаланувчилар бўлинувчи сирни ўзаро эмас, балки 1-@ ва 2-@ схемалари бўйича яратадилар, чунки улар ўзларининг махфий калитларидан ва нияти бузуқ одам @нинг очиқ калити $K_@$ дан фойдаланадилар.



9.1-расм. "Man-in-the-middle" атакасини амалга ошириш.

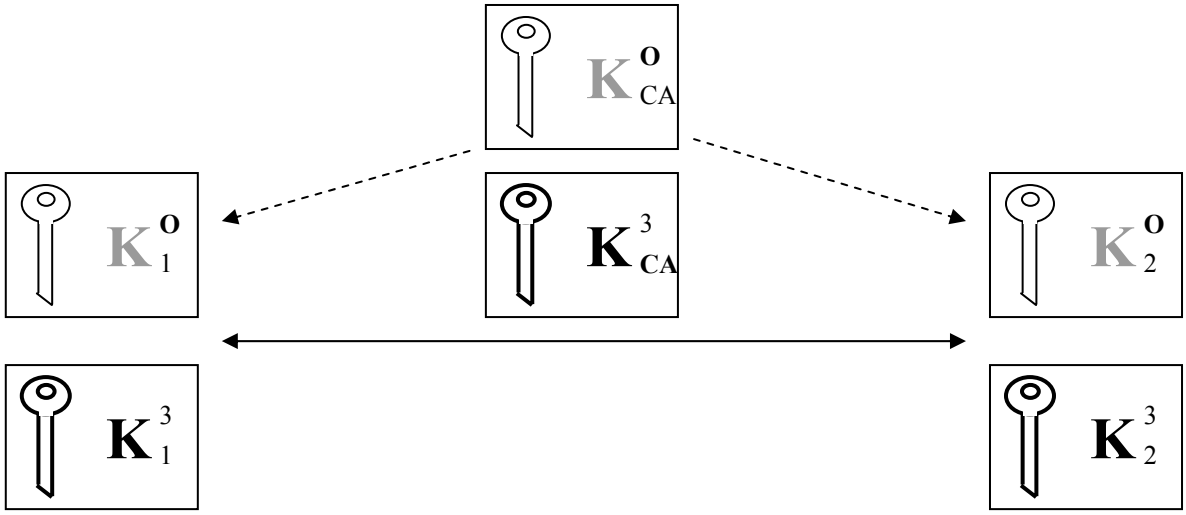
1-фойдаланувчи 2-фойдаланувчига шифрланган ахборотни жунатган вақтида нияти бузуқ одам @ уни ушлаб қолиши ва расшифровка қилиши мумкин (унда 1-фойдаланувчи билан бўлинувчи сир $K_{1@}$ бор). Сўнгра нияти бузуқ одам @ ахборотни (ўзгартирилгани бўлиши мумкин) ўзи ва 2-нчи фойдаланувчи ҳисоблаган бўлинувчи сир $K_{@2}$ дан фойдаланиб янгидан шифрлайди. Натижада 2-фойдаланувчи 1-фойдаланувчи билан ҳимояланган каналга эгаман деб ўйлаб, нияти бузуқ одам жўнатган ахборотни олади, расшифровка қилади ва ишлатади.

Бу хужумга қарши самарали восита нотариус ёки сертификациялаш идораси CA (Certificate Authority). Очиқ калитларнинг нотариал тасдиқланган сертификатларини қўллаш man-in-the-middle хужумини олдини олишга имкон беради.

1-фойдаланувчи нотариусга боради, нотариус 1-фойдаланувчининг очиқ калитини ўзининг маҳфий калитидан фойдаланиб, электрон рақамли имзоси билан имзолайди. Бунда нотариус рақамли имзоси билан нафақат 1-фойдаланувчининг очиқ калитини, балки фойдаланувчи хусусидаги қатор аниқ ахборотни (Ф.И.Ш., иш жойи ва ҳ.) ҳамда имзонинг таъсир муддатини имзолайди. Ҳосил бўлган хужжат (файл) 1-фойдаланувчи *очиқ калитининг сертификати* деб аталади. Нотариусдан ўзининг очиқ калити учун сертификат олишнинг худди шу муолажасини 2-фойдаланувчи ҳам бажаради.

1 ва 2-фойдаланувчи имзо чекилган очиқ калитларини алмашишганидан сўнг, улар нотариуснинг электрон рақамли имзосини ва сертификат ҳақиқатан 1- ёки 2- фойдаланувчига берилганлигини текширади. Нотариуснинг электрон рақамли имзосини текшириш фойдаланувчилар нотариусга ташриф буюрганларида эҳтиётдан олиб қуйилган нотариусни очиқ калити ёрдамида шеригидан олган сертификатни расшифровка қилиш орқали бажарилади. Натижада нотариус СА орқали фойдаланувчилар орасида оддий ишонч занжири пайдо бўлади (9.2-расм).

Нияти бузуқ одам @ нотариусга бориб 1-фойдаланувчининг сертификатини ололмайди, чунки унга бу сертификатни олиш вақтида паспортини кўрсатишига ва у 1- фойдаланувчи эканлигини исботлашига тўғри келади.



9.2-расм. Нотариус СА орқали фойдаланувчилар орасидаги оддий ишонч занжири

Очиқ калит сертификатлари. Очиқ калит сертификатларини шакллантириш X.509 стандарт тарафидан тавсия этилган *қатъий аутентификациялаш* принципига ва очиқ калитли криптотизим хусусиятларига асосланади.

Очиқ калит сертикати деганда маълумотлар бўлими ва имзо бўлимидан ташкил топган маълумотлар тузилмаси тушунилади. Маълумотлар бўлимида очиқ калит хусусидаги ва калит эгасини идентификацияловчи маълумотлар бўлади. Имзо бўлимида очиқ калитли маълумотлар бўлими учун генерацияланган очиқ калит эгасини аутентификацияловчи электрон рақамли имзо бўлади. Сертификация маркази СА сертификатлардаги очиқ

калитларни аутентификациялашни таъминловчи ишончли учинчи томон ҳисобланади.

Сертификациялаш маркази ўзининг жуфт (очиқ-махфий) калитига эга бўлиб, махфий калит сертификатларни имзолаш учун ишлатилса, очиқ калит чоп этилади ва ундан фойдаланувчилар сертификатдаги очиқ калитнинг ҳақиқийлигини текширишда фойдаланадилар. Таъкидлаш лозимки, сертифкация марказининг очиқ калитини хавфсиз узатиш нафақат сертифкация марказига шахсан мурожаат асосида, балки бу очиқ калитни керакли ваколатга эга бўлган бошқа сертифкация маркази томонидан сертификациялаш асосида ҳам амалга ошириш мумкин. Сертификация маркази фойдаланувчининг очиқ калити сертификатини маълумотларнинг маълум тўпламини рақамли имзо билан тасдиқлаш орқали шакллантиради.

Одатда, маълумотларнинг бу тўпламига қуйидагилар киради:

- очиқ калитнинг таъсир даври: даврининг бошланиши ва ниҳояси саналарини ўз ичига олади;

- калитнинг номери ва серияси;

- фойдаланувчининг ноёб исми;

- фойдаланувчининг очиқ калити хусусидаги ахборот: ушбу калит аталган алгоритмнинг идентификатори ва очиқ калитнинг ўзи;

- электрон рақамли имзони текшириш муолажасида ишлатилувчи алгоритм (масалан, электрон рақамли имзони генерацияловчи алгоритм идентификатори);

- сертификация марказининг ноёб исми;

Очиқ калит сертификати қуйидаги хусусиятларга эга:

- сертификация марказининг очиқ калитидан фойдаланувчининг ҳар бири сертифкатга киритилган очиқ калитни чиқариб олиши мумкин;

- сертифкация марказидан ташқари ҳеч бир томон сертификатни билинтирмасдан ўзгартираолмайди (сертификатларни сохталаштириш мумкин эмас).

Сертифкатларни сохталаштириш мумкин эмаслиги, уларни умумфойдаланувчи маълумотномаларда, ҳимояламасдан чоп этишга имкон туғдиради.

Очиқ калит сертифкатини яратиш жуфт калитни (очиқ-махфий) яратишдан бошланади. Калитни генерациялаш муолажаси қуйидаги иккита усул орқали амалга оширилиши мумкин:

- сертификация маркази калитлар жуфтини яратади. Очиқ калит сертифкатга киритилади, унинг жуфти-махфий калит эса фойдаланувчига узатилади (фойдаланувчини аутентификациялашни ва калит узатилишининг конфиденциаллигини таъминлаган ҳолда).

- фойдаланувчи калитлар жуфтини ўзи яратади. Махфий калит фойдаланувчида сақланади, очиқ калит эса ҳимояланган канал орқали сертифкация марказига юборилади.

Ҳар бир фойдаланувчи сертифкация маркази томонидан шаклланти-рилган битта ёки бир нечта калитларнинг эгаси бўлиши мумкин. Фойдаланувчи бир неча турли сертифкация марказидан олинган сертификатларга ҳам эга бўлиши мумкин.

Амалда бошқа сертификация марказидан сертифкат оладиган фойдаланувчиларни аутентификациялаш эҳтиёжи туғилади.

Сертификатларни бошқариш тизимларининг базавий тузилмалари. Сертифкатларни бошқариш тизими-ўзаро ахборот алмашишда хавфсизликни таъминлаш мақсадида очиқ калитли криптографик технологиялардан фойдаланишга зарур бўлган дастурий-аппарат воситалари ҳамда ташкилий-техник тадбирлар комплекси.

Очиқ калитларни бошқариш инфратузилмаси PKI man-in-the-middle хужумларидан ишончли ҳимоялашни амалга оширишга имкон берувчи нотариуслар тармоғидан иборат. Нотариус орқали фойдаланувчилар орасидаги оддий ишонч занжири (9.2-расм) битта нотариусга, унга ташриф буюрган фойдаланувчиларнинг очиқ калитларини, имзоланган сертификатларни яратиш йўли билан ҳимоялашга имкон беради.

Бу тизимнинг самарали ишлаши қуйидагиларга боғлиқ:

- ўзаро алоқа иштирокчилари сертификация маркази очиқ сертификатининг ҳақиқий нусхасига эга бўлишлари шарт;

- ўзаро алоқа иштрокчилари ишлатадиган ахборотни ҳимоялаш воситалари ўзаро алоқадаги шеригининг ҳар қандай сертификатини сертифика-

ция марказининг очиқ сертификатидан фойдаланиб автоматик тарзда текшира олиши лозим.

Баъзида ўзаро алоқадаги шериклар сертификация марказидан жуда узоқда бўлишлиги мумкин. Бу ҳолда СА нотариусларининг тақсимланган қатламлари яратилади.

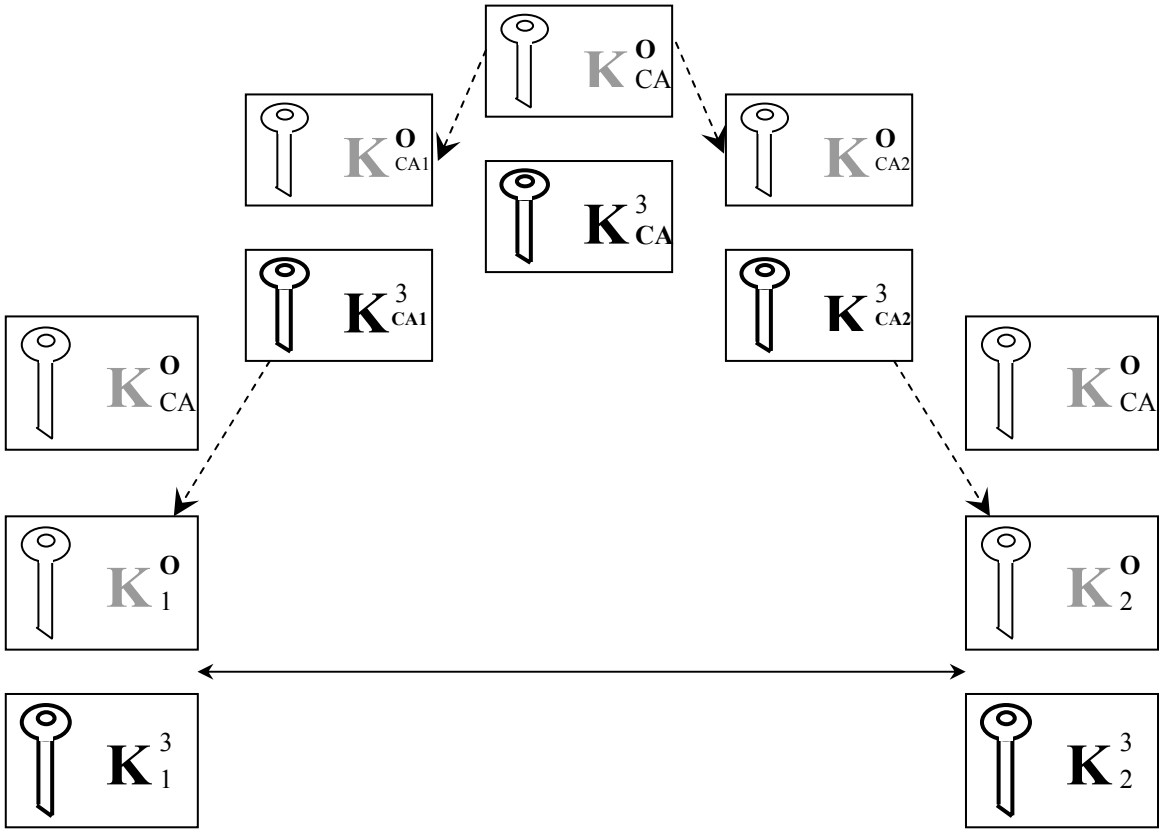
Сертификациялашнинг учта базавий модели фарқланади:

- сертификатларнинг иерархик (шажара) занжирига асосланган сертификациялашнинг иерархик модели;

- кросс-сертификациялаш модели (ўзаро сертификациялашни кўзда тутади);

- сертификациялашнинг тармоқ (гибрид) модели (иерархик ва ўзаро сертификациялаш элементларини ўз ичига олади);

Иерархик моделда СА лар бошқа СА ларга сертификатлар берувчи илдиз сертификация марказига иерархик тобеликда жойлашган (9.3-расм).



9.3-расм. САнинг икки сатҳли иерархияси

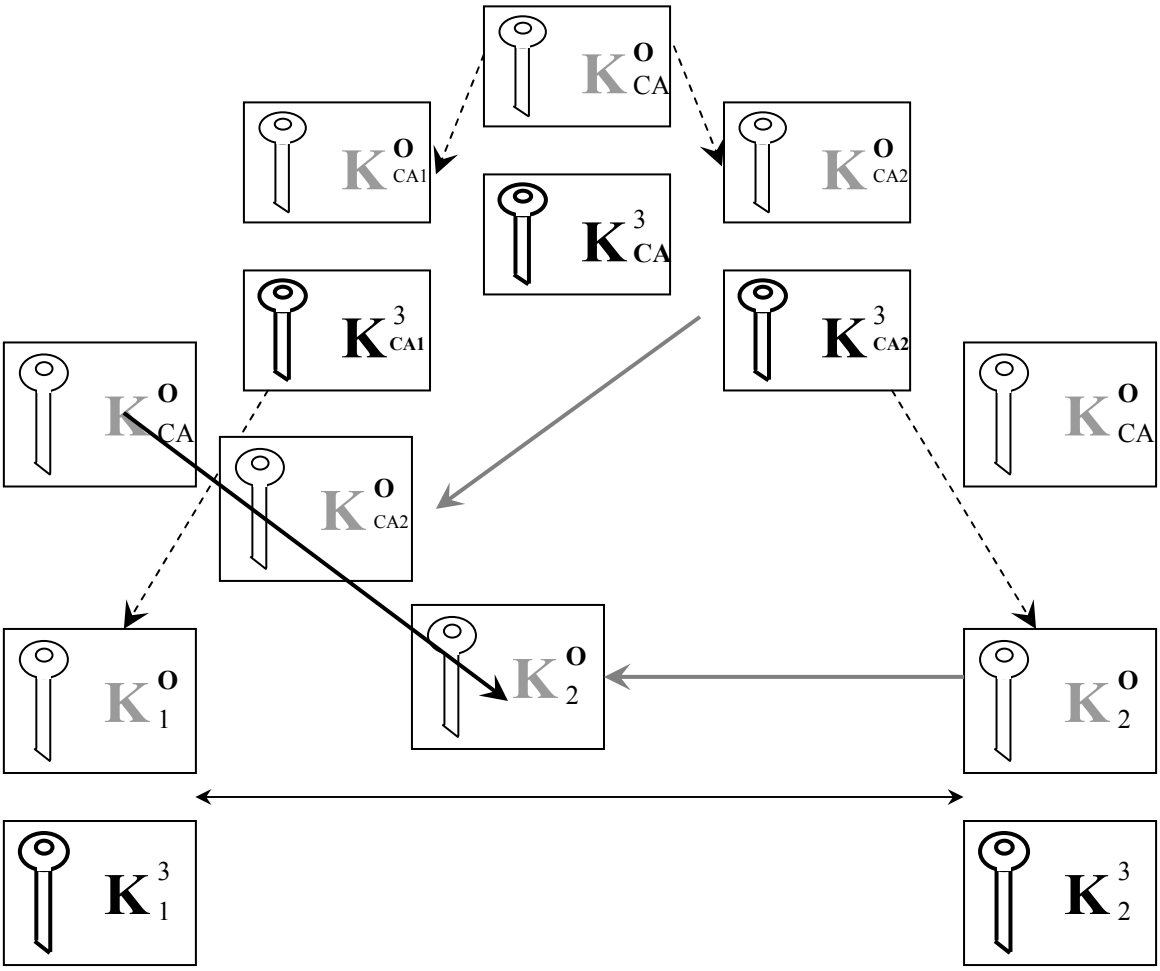
Илдиз сертификация марказининг вазифаси тобе СА1 ва СА2ларни қайдлашдан иборат. Ҳар бир СА хавфсизликнинг ягона даражасини

таъминлаш мақсадида сертификациялашнинг берилган сиёсатига мувофиқ ишлайди. 9.3–расмда келтирилган мисолда СА нотариусларнинг яна бир иерархик сатҳи яратилади. Нотариуслар:

- фойдаланувчиларга ўхшаб сертификатларини марказий САда имзолашади;

- марказий САга ўхшаб оддий фойдаланувчиларнинг сертификатларини махфий калитлари билан, имзолайдилар.

Масофадаги шерикнинг ҳақиқийлигини текшириш мантиқи қуйидагиича қурилади (9.4-расм)



9.4-расм. Масофадаги абонент сертификатини текшириш схемаси.

- фойдаланувчи шеригининг сертификатини олиб, уни нотаниш СА имзолаганини аниқлайди;

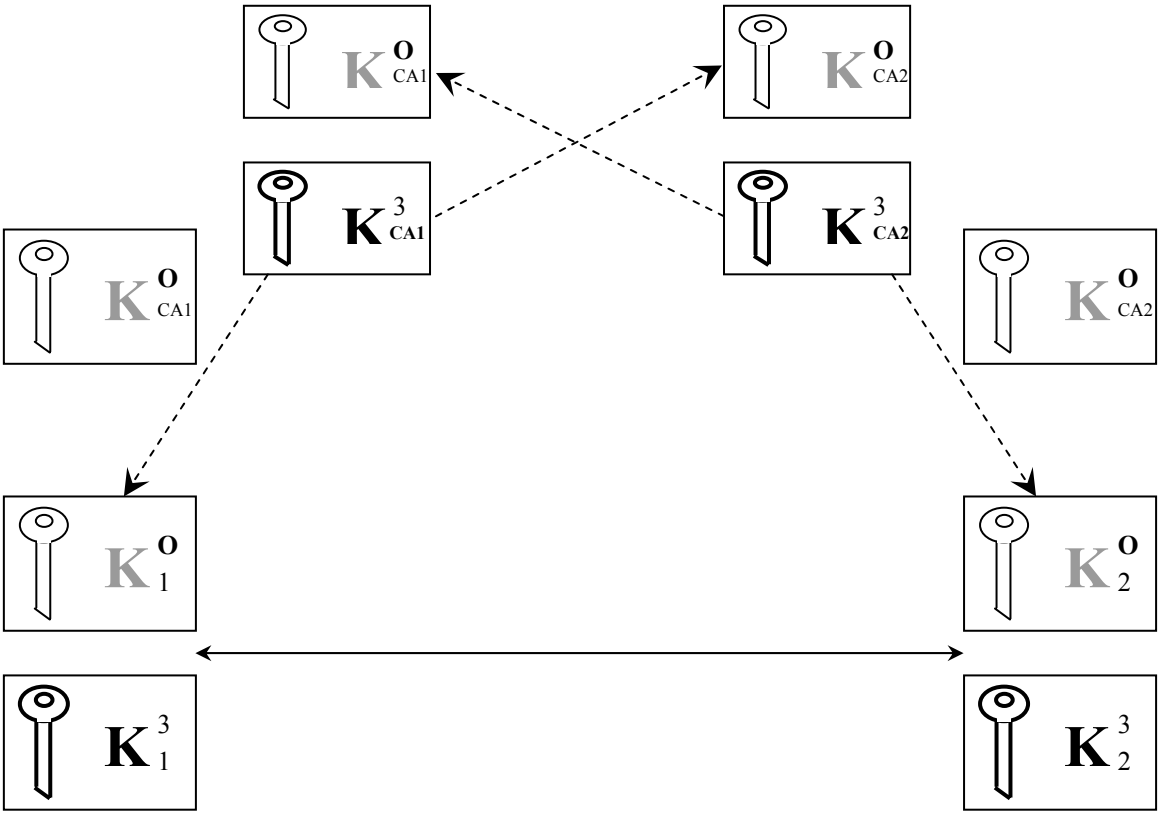
- у шеригидан ушбу САнинг сертификатини сурайди;

- САнинг сертификатини олиб, уни марказий СА сертификати билан текширади;

- муваффақиятли текширишдан сўнг фойдаланувчи бу САга ишона бошлайди ва унинг сертификати билан масофадаги фойдаланувчи сертификатини текширади.

Худди шундай текширишни иккинчи шерик ҳам бажаради. Муҳими, ишлатиладиган ахборотни ҳимоялаш тизимлари бундай мураккаб иерархик текширишларни автоматик тарзда бажараолсинлар. Тавсифланган иерархик схемани, зарурият туғилганда иерархиянинг янги сатҳларини киритиб, давом эттириш мумкин.

Кросс-сертификациялаш моделида иерархиянинг бир шоҳида бўлмаган мустақил САлар сертификация марказлари тармоғида ўзаро сертификацияланадилар. Текшириш схемаси ўзгармайди, чунки фойдаланувчига бегона нотариус унинг нотариусига тобедек туюлади (9.5-расм).



9.5-расм. Кросс-сертификатлаш схемаси.

Таъкидлаш лозимки, кросс-сертификациялаш модели сертификатларни бошқариш тизимининг тармоқли архитектурасининг хусусий ҳоли ҳисобланади.

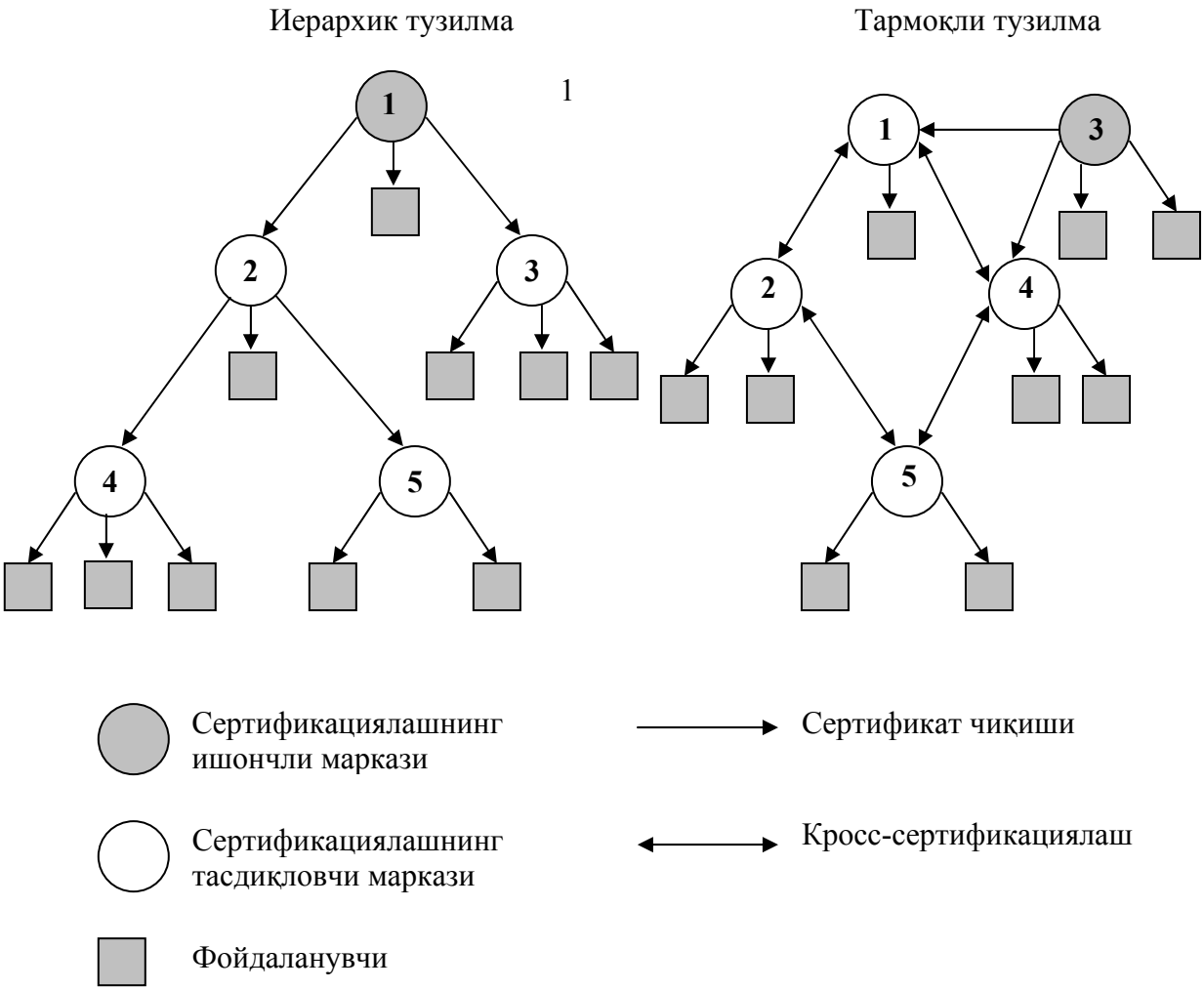
Сертификатларни бошқариш тизимининг иерархик ва тармоқ архитектураларининг умумлаштирилган схемалари 9.6-расмда келтирилган.

Сертификатларни бошқариш тизимининг *иерархик тузилмаси* қуйидаги афзалликларга эга:

- у мавжуд федерал ва идора ташкилий-бошқарув тузилмаларга ўхшаш ва уларнинг принциплари бўйича қурилиши мумкин;

- у исмларнинг иерархик дарахтига осонгина боғланиши мумкин;

- у ўзаро алоқадаги барча томонлар учун сертификатлар занжирини қидириш, қуриш ва верификациялашнинг оддий алгоритмини аниқлайди;



9.6–расм. Сертификатларни бошқариш тизимининг иерархик ва тармоқли архитектуралари

- иккита фойдаланувчининг ўзаро алоқани таъминлаши учун улардан бирининг иккинчисига ўзининг сертификатлар занжирини тақдим этиши кифоя, бу ўзаро алоқа билан боғлиқ муаммоларни камайтиради.

Иерархик архитектурага қуйидаги камчиликлар характерли:

- барча охирги фойдаланувчиларнинг ўзаро алоқани таъминлаш учун фақат битта илдизли ишончли СА бўлиши шарт;

- тижорат тузилмаларининг ўзаро алоқаси иерархикдан кўра кўпроқ тўғри характерга эга.

Сертификататларни бошқариш тизимининг *тармоқ архитектураси* қуйидаги афзалликларга эга:

- у анчагина мослашувчан ва замонавий бизнесда мавжуд бўлган бевосита ишончли ўзаро муносабатларнинг ўрнатилишига имкон беради;

- охирги фойдаланувчи ҳеч бўлмаганда унинг сертификатини босиб чиқарган марказга ишониши шарт ва тизимдаги ишонч муносабатлари мана шунга асосланган;

- фойдаланувчилари ўзаро тез-тез алоқа қилувчи турли тасдиқловчи САларни бевосита кросс-сертификациялаш мумкин, бу занжирларни верификациялаш жараёнини қисқартиради;

- тасдиқловчи СА калити обрўсизлантирилганидан сўнг тиклаш жараёни иерархик тузилмага қараганда тармоқ тузилмасида оддийроқ.

Аммо сертификатларни бошқаришнинг тармоқ архитектураси қуйидаги камчиликларга эга:

- барча ўзаро алоқа томонлар учун сертификатлар занжирини қидириш ва қуриш алгоритми жуда мураккаб бўлиши мумкин;

- фойдаланувчи унинг сертификатини бошқа барча фойдаланувчилар томонидан текширилишини таъминловчи занжирни тақдим этаолмайди.

Эҳтимол, яқин орада сертификациялаш иерархиясининг энг юқори сатҳида турли ташкилотларнинг ишонч занжирлари алоқасини таъминловчи давлат нотариуси бўлиши лозим.

9.2. Очиқ калитларни бошқариш инфратузилмасининг мантиқий тузилмаси ва компонентлари

Очиқ калитларни бошқариш инфратузилмаси PKIнинг асосий вазифалари қуйидагилар:

- рақамли калитлар ва сертификатларнинг ҳаёт циклини мададлаш (яъни калитларни генерациялаш, сертификатларни яратиш ва имзолаш, уларни тақсимлаш ва ҳ.);

- обрўсизлантириш фактларини қайдлаш ва чақириб олинган сертификатларнинг "қора" руйхатини чоп этиш;

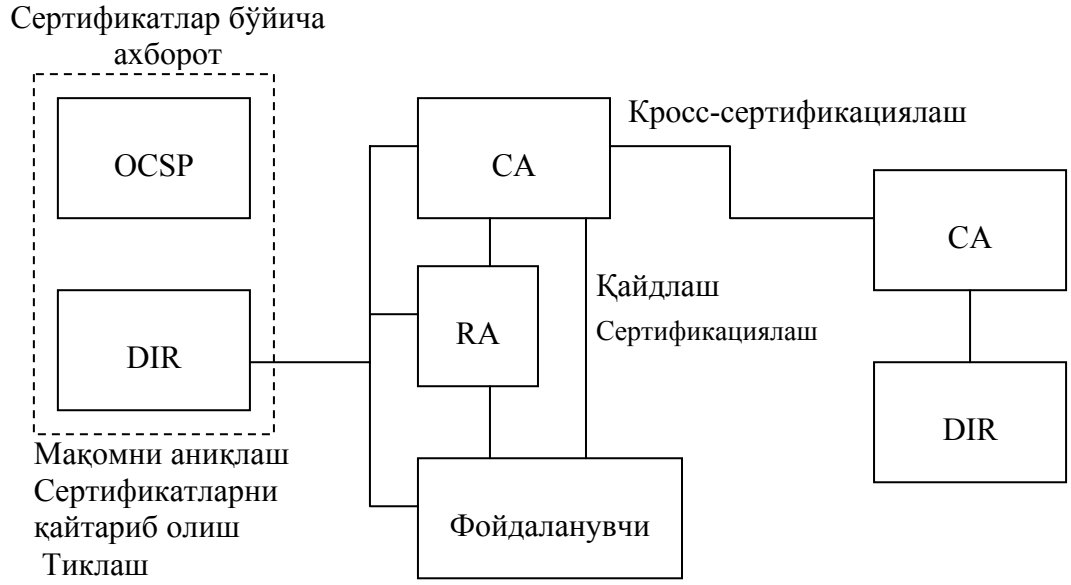
- фойдаланувчининг тизимдан фойдаланиш вақтини имкони борича камайтирувчи идентификациялаш ва аутентификациялаш жараёнларини мададлаш:

- мавжуд иловалар ва хавфсизлик қисм тизимининг барча компонентларини интеграциялаш механизмини (PKIга асосланган) амалга ошириш;

- барча фойдаланувчилар ва иловалар учун бир хил ва таркибида барча зарурий калит компонентлари ва сертификатлар бўлган хавфсизликнинг ягона токенидан фойдаланиш имкониятини тақдим этиш.

Хавфсизлик токени – фойдаланувчининг тизимдаги барча хуқуқлари ва қуршовини аниқловчи хавфсизликнинг шахсий воситаси, масалан смарт-карта.

9.7-расмда очиқ калитларни бошқариш инфратузилмасининг мантиқий тузилмаси ва асосий компонентлари келтирилган.



9.7–расм. PKIнинг мантиқий тузилмаси ва асосий компонентлари

Расмда қуйидаги белгилашлар қабул қилинган:

- CA сертификациялаш маркази;

- RA – қайдлаш маркази;

- OCSP – жорий сертификат мақомининг протоколи (Online Certificate Status Protocol);

- DIR – X.511, X.519, DAP, LDAP фойдаланиш протоколлари бўйича диркетория хизмати.

Қайдлаш маркази RA – PKI элементи, қайдлашни амалга оширувчи вакил, яъни фойдаланувчига сертификатни ҳимояланган ҳолда бериш имкониятини таъминлаш мақсадида фойдаланувчиларни аутентификациялашни ва уларни қайдлашни амалга оширади. Қайдлаш марказининг хусусияти шундай иборатки, у функционал нуқтаи назаридан сертификация марказига қараганда фойдаланувчига яқинроқ. Ундан ташқари айнан қайдлаш маркази PKIнинг ўзаро алоқага лаёқатлигини таъминловчи самарали интерфейс ҳисобланади.

Сертификация маркази CA – PKIнинг элементи (сертификатларнинг ишончли манбаи, нотариус), унга сертификатларни яратиш ва/ёки тасдиқлаш ишониб топширилган. Сертификация марказининг ишлаш схемаси қуйидагича:

- CA шахсий калитларини генерациялайди ва фойдаланувчилар сертификатларини текширишга аталган CA сертификатларини шакллантиради;

- фойдаланувчилар сертифкациялашга сўровларни шакллантирадилар ва уларни у ёки бу усул бўйича CAга етказади;

- CA фойдаланувчилар сўровлари асосида уларнинг сертификатларини шакллантиради;

- CA бекор қилинган сертификатлар руйхатларини (CRL) шакллантиради ва вақти-вақти билан янгилайди;

- фойдаланувчи сертификатлари, CA сертификатлари ва бекор қилинганлар руйхати CRL сертификатлар маркази томонидан чоп этилади (фойдаланувчиларга тарқатилади ёки умумфойдаланувчи маълумотномага жойлаштирилади).

PKI бажарадиган функцияларни шартли равишда бир неча гурухларга ажратиш мумкин:

- сертификаталарни бошқариш функциялари;

- калитларни бошқариш функциялари;

- қўшимча функциялар (хизматлар).

Сертификаталарни бошқариш функцияларига қуйидагилар киради:

- *қайдлаш.* Нафақат функцияларнинг бир қисми, балки PKIнинг хавфсизлиги ҳам тўғри қайдлашга ва идентифкациялашга асосланган. Фойдаланувчилар сифатида физик фойдаланувчилар, татбиқий дастур, тармоқ қурилмаси ва ҳ. иштирок этиши мумкин. Идентификациялашда ишлатиладиган усулларни сертифкациялаш сиёсати белгилайди. Шундай қилиб, фойдаланувчиларни идентификациялаш ва қайдлаш PKI тизимининг минимал тўлиқ компонентлари ҳисобланади;

- *очиқ калитларни сертификациялаш.* Сертификациялаш жараёнига сертифкациялаш маркази CA жавоб беради. Моҳиятан, сертификациялаш жараёни фойдаланувчи исмини очиқ калит билан боғлашдан иборат.

CA қуйидаги ҳаракатларни бажарган ҳолда фойдаланувчи ва пастроқ сатҳдаги CA сертификатларини имзолайди:

- фойдаланувчиларнинг ҳақиқийлигини текшириш;
- сертифкатга идентификатор бериш;
- маълумотларни сертифкатга киритиш;
- ҳаракат вақтини (бошланиш-ниҳояси) ўрнатиш;
- сертификатни имзолаш;
- сертифкатни сертификатларнинг очиқ серверида чоп этиш.

CAнинг махфий калитини сақлаш. Бу тизимнинг энг нозик нуқтаси. CA махфий калитини *обрўсизлантирилиши* унинг ихтиёридаги бутун тизимни бузади. CAнинг махфий калити жойлашган компьютер ишончли қўриқланиши лозим;

- *сертификатлар базасини сақлаш ва сертифкатларни тақсимлаш.* Тизим ишлашининг қулайлигини таъминлаш мақсадида фойдаланувчиларнинг ва оралиқ CAларнинг (энг юқори сатҳ CAсидан бўлак) барча сертифкатлари сертификатлар сервери деб аталувчи умумфойдаланувчи серверга олиб қўйилади. Бу ҳолда фойдаланувчилар абонентнинг сертификатини, ҳатто у тармоқда вақтинча бўлмаган ҳолда ҳам, олишлари мумкин;

- ***сертификатни янгилаш.*** Ушбу жараён сертификат таъсири муддати ўтган ҳолда фаоллашади ва фойдаланувчи очиқ калити учун янги сертификатни беришдан иборат бўлади. Агар калитлар жуфти обрўсизлантирилган бўлса ёки янги сертификат сиёсат, кенгайиш ёки хусу-

сият атамаларида олдингисидан фарқланса бу усул ишлатилмайди. Яроқчилик муддати даврида сертификатнинг исми ва мансублиги (фойдаланувчининг бошқа бўлимга ўтиши) каби жиддий бўлмаган хусусиятларининг ўзгариши ҳам сертификатни олдинги очиқ калит билан янгилашни (регенерациялашни) талаб этишга олиб келиши мумкин.

- ***калитларни янгилаш.*** Фойдаланувчилар ёки учинчи томон калитларнинг янги жуфтини генерациялаганларида янги очиқ калитга мос келувчи сертификатни яратиш зарур. Бу усулдан сертификатни янгилаш мумкин бўлган ҳолларида ҳам фойдаланилади;

- ***сертификатни қайтариб олиш мақомини аниқлаш.*** Ушбу жараён фойдаланувчига сертификатининг қайтариб олинган эмаслигини текширишга имкон беради. Бу жараён сертификатнинг очиқ калитлар каталоги PKDда (Public Key Directory) ва сертификатларни қайтариб олиш руйхати CRLда (Certificate Revocation List) борлигини текшириш орқали ёки бу масалани ечишга ваколати бўлган учинчи томонга сўров ёрдамида ташкил этилиши мумкин.

- ***сертификатни қайтариб олиш.*** Бу жараён турли ҳолатлар натижасида хавфсизликнинг муайян сиёсатига боғлиқ ҳолда (масалан, калитларнинг обрўсизлантирилиши, исмларнинг ўзгариши, фойдаланишнинг тўхташи ва ҳ.) бўлиши мумкин.

- ***калитларни бошқариш функцияси*** – калитларни генерациялаш ва тақсимлаш асосий қисм гуруҳларига бўлинади.

Калитларни тақсимлаш функциялари ўз навбатида очиқ калитларни тақсимлаш ва токенларни персоналлаштиришга бўлинади.

Токенларни персоналлаштиришда физик қурилмалар – токенлардан фойдаланиб махфий калитларни ва қўшимча маълумотларни сақлаш ташкил этилади; токенларнинг персонализацияси CA, RA ва фойдаланувчи томонидан мададланиши лозим. Масалан, смарт-картанинг персонализацияси ўрнатиш (файл тизимини яратиш) муолажасини, тасодифий PIN-кодни ёки паролни танлаш, бу смарт-картага тегишли барча маълумотларни етказиш ва сақлашни ўз ичига олиши мумкин.

Қўшимча функциялар (хизматлар) гуруҳи таркибига қуйидагилар киради:

- ўзаро сертификациялаш (турли САларда кросс-сертификациялаш);

- очиқ калитни унинг унга қуйиладиган арифметик талабларга мос келишини, яъни очиқ калит ҳақиқий эканлигини текшириш;

- сертификатни текшириш; агар фойдаланувчи бошқа фойдаланувчининг рақамли имзосига ишонишни ҳоҳласа ва мос сертификатни текшираолмаса, текширишни ишончли учинчи томондан илтимос қилиши мумкин;

- архивлаш хизматлари ва ҳ.

Очиқ калитлар инфратузилмаси PKI қуйидаги қатор иловалар ва стандартларни мададлайди:

- очиқ калит сертификатларини мададловчи воситалар ўрнатилган Linux, FreeBSD, HP-UX, Microsoft Windows, Novell Netware, Sun Solaris операцион тизимлари;

- очиқ калит сертификатлари асосида фойдаланувчиларни аутентификациялаш механизмини мададловчи маълумотлар базасини бошқариш тизимлари, хусусан Oracle, DB2, Informix, Sybase;

- IP протоколи асосида амалга оширилувчи виртуал ҳимояланган тармоқларни (VPN) ташкил этиш воситалари, хусусан Cisco Systems, Nortel Network компанияларининг телекоммуникация асбоб-ускуналари, ҳамда ихтисослаштирилган дастурий таъминот.

- электрон хужжат айланиши тизимлари, масалан Lotus Notes, Microsoft Exchange, ҳамда ҳимояланган почта алмашиш стандарти S/MIMEни мададловчи почта тизимлари;

- Microsoft Active Directory, Novell NDS, Netscape iPlanet каталогларининг хизмати;

- SSL стандарти асосида амалга оширилувчи Web-ресурслардан фойдаланиш тизимлари.

- фойдаланувчиларни аутентификациялаш тизимлари, хусусан RSA компаниясининг SecurID ва ҳ.

Ўз навбатида, очиқ калитлар инфратузилмаси санаб ўтилган функционал соҳаларни интеграциялаши мумкин. Натижада, очиқ калитлар ин-

фратузилмаларини компания ахборот тизимига интеграциялаш ва умумий стандартлар ва очиқ калит сертификатларидан фойдаланиш йўли билан ахборот хавфсизлигининг комплекс тизимини яратиш мумкин.

Юқорида келтирилганлар очиқ калитлар инфратузилмасини яратиш ва мададлаш хизматлари аҳамиятини ошишига олиб келади.

X боб. АХБОРОТ-КОММУНИКАЦИОН ТИЗИМЛАРДА СУҚИЛИБ КИРИШЛАРНИ АНИҚЛАШ

10.1. Хавфсизликни адаптив бошқариш концепцияси

Ташкилотларда ҳимоялаш билан боғлиқ бўлган муаммоларни ечиш учун аксарият ҳолларда қисман ёндашишлардан фойдаланишади. Бу ёндашишлар, одатда, аввало фойдалана олувчи ресурсларнинг жорий даражаси орқали аниқланади. Ундан ташқари, хавфсизлик маъмурлари кўпинча ўзларига тушунарли бўлган хавфсизлик хавф-хатарларига реакция кўрсатишади. Аслида хавф-хатарлар жуда кўп бўлиши мумкин. Корпоратив ахборот тизимини фақат қатъий жорий назорати ва хавфсизликнинг умумий сиёсатини таъминловчи комплекс ёндашиш хавфсизлик хавф-хатарларини анчагина камайтириши мумкин.

Охирги вақтда турли компаниялар томонидан қатор ёндашишлар ишлаб чиқилдики, бу ёндашишлар нафақат мавжуд заифликларни аниқлашга, балки ўзгарган эски ёки пайдо бўлган янги заифликларни аниқлашга ва уларга мос ҳимоялаш воситаларини қарши қўйишга имкон беради. Хусусан, ISS(Internet Security Systems) компанияси томонидан *хавфсизликни адаптив бошқариш модели* ANS (Adaptive Network Security) ишлаб чиқилди.

Хавфсизликка адаптив ёндашиш, тўғри лойиҳаланган ва яхши бошқарилувчи жараён ва воситалар ёрдамида хавфсизлик хавф-хатарларини реал вақт режимида назоратлаш, аниқлаш ва уларга реакция кўрсатишга имкон беради.

Тармоқнинг адаптив хавфсизлиги қуйидаги асосий учта элемент орқали таъминланади:

- хавф-хатарларни баҳолаш;
- ҳимояланишни таҳлиллаш;
- хужумларни аниқлаш.

Хавф-хатарларни баҳолаш. Хавф-хатарларни (келтирадиган зарарнинг жиддийлик даражаси бўйича), тармоқ қисм тизимларини (жиддийлик даражаси бўйича), таҳдидларни (уларнинг амалга оширилиши эҳтимоллиги

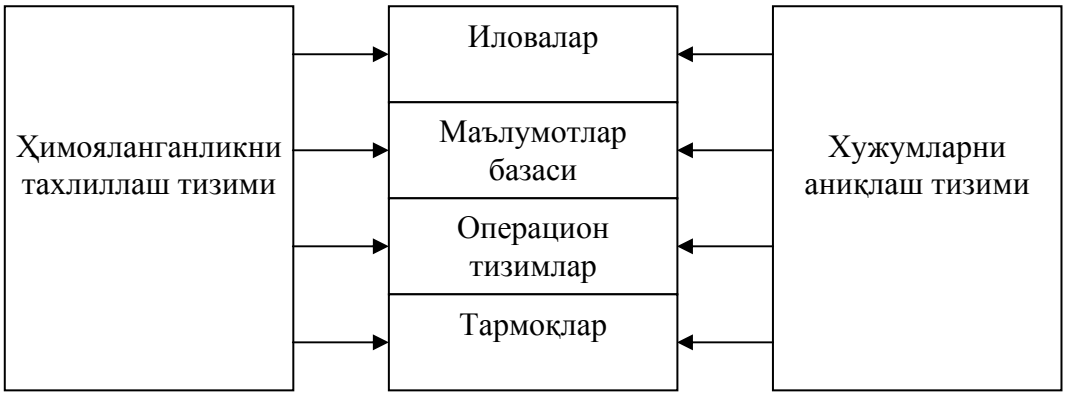
бўйича) аниқлаш ва рутбалашдан иборат. Тармоқ конфигурацияси муттасил ўзгариши сабабли, хавф-хатарларни баҳолаш жараёни ҳам узлуксиз ўтказилиши лозим. Корпоратив ахборот тизимининг ҳимоялаш тизимини қуриш хавф-хатарларни баҳолашдан бошланиши лозим.

Ҳимояланишни тахлиллаш – тармоқнинг заиф жойларини қидириш. Тармоқ уланишлардан, узеллардан, хостлардан, ишчи станциялардан, иловалардан ва маълумот базаларидан таркиб топган. Буларнинг барчаси ҳимояланишлар самарадорлигининг ҳамда ноъмалум заифликларининг аниқланишига муҳтож. Ҳимояланишни таҳлиллаш технологияси тармоқни тадқиқлаш, нозик жойларини топиш, бу маълумотларни умумлаштириш ва улар бўйича ҳисобот бериш имкониятига эга. Агар бу технологияни амалга оширувчи тизим адаптив компонентга ҳам эга бўлса, аниқланган заифликларни автоматик тарзда бартараф этиш мумкин. Ҳимояланишни тахлиллаш технологияси тармоқ хавфсизлиги сиёсатини, уни ташкилот ташқарисидан ёки ичкарисидан бузишга уринишлардан олдин, амалга оширишга имкон берувчи таъсирчан усул ҳисобланади.

Ҳимояланишни тахлиллаш технологияси томонидан идентификацияланувчи муаммоларнинг баъзилари қуйидагилар:

- тизимлардаги "тешиклар" (back door) ва троян оти хилидаги дастур;
- кучсиз пароллар;
- ҳимояланмаган тизимдан суқилиб киришга ва "хизмат қилишдан воз кечиш" хилидаги хужумларга таъсирчанлик;
- операцион тизимлардаги зарурий янгиланишларнинг йўқлиги;
- тармоқлараро экранларнинг, Web-серверларнинг ва маълумотлар базасининг нотўғри созланиши ва ҳ.

Хужумларни аниқлаш – корпоратив тармоқдаги шубҳали харакатларни баҳолаш жараёни. Хужумларни аниқлаш операцион тизим ва иловаларни қайдлаш журналларини ёки реал вақтдаги трафикни тахлиллаш орқали амалга оширилади. Тармоқ узеллари ёки сегментларида жойлаштирилган хужумларни аниқлаш компонентлари турли ходисаларни, хусусан, маълум заифликлардан фойдаланувчи ҳаракатларни ҳам баҳолайди (10.1-расм).



10.1-расм. Ҳимояланганликни тахлиллаш ва хужумларни аниқлаш тизимларининг ўзаро алоқаси

Хавфсизликни адаптив бошқариш модели ANSнинг адаптив компоненти, янги заифликлар хусусидаги энг охирги ахборотни тақдим қилган ҳолда, ҳимояланишни таҳлиллаш жараёнини модификациялашга жавоб беради. У хужумларни аниқлаш компонентини ҳам, уни хужумлар хусусидаги охирги ахборот билан тўлдириш орқали, модификациялайди. Адаптив компонентнинг мисоли сифатида янги вирусларни аниқлаш учун вирусга қарши дастурнинг маълумотлар базасини янгилаш механизмини кўрсатиш мумкин.

Хавфсизликни адаптив бошқариш моделидан (10.2-расм) фойдаланиш

10.2–расм. Хавфсизликни бошқариш адаптив (мослашувчан) модели

барча таҳдидларни назоратлаш ва уларга ўз вақтида самарали реакция кўрсатиш имконини беради. Бу эса ўз навбатида, нафақат таҳдидларнинг амалга оширилишига сабаб бўлувчи заифликларни бартараф қилишга, балки заифликлар пайдо бўлиш шароитларини таҳлиллашга имкон беради.

Тармоқ хавфсизлигини адаптив бошқариш модели тармоқда суиистеъмол қилишни камайтиришга, тармоқдаги ходисалардан фойдаланувчилар, маъмурлар ва компания раҳбариятининг хабардорлик даражасини ошишига ҳам имкон беради. Таъкидлаш лозимки, ушбу модель олдин ишлатилувчи ҳимоялаш механизмларидан (фойдаланишни чегаралаш, аутентификациялаш ва ҳ.) воз кечмайди. Уларнинг функционаллигини янги технология эвазига кенгайтиради. Ўзларининг ахборот хавфсизлигини таъминлаш тизимларини замонавий талабларга мос келишини хохловчи ташкилотлар мавжуд ечимларни учта янги компонент-ҳимояланишни тахлиллаш, хужумларни аниқлаш ва хавф-хатарни баҳолаш билан тўлдириши лозим.

10.2. Ҳимояланишни тахлиллаш

Ҳимояланишни тахлиллаш воситалари заифликларни топиб ва ўз вақтида йўқ қилиб хужумни амалга ошириш имкониятини бартараф қилади. Натижада, ҳимоялаш воситаларини ишлатилишига бўладиган барча сарф-ҳаражатлар камаяди.

Ҳимояланишни тахлиллаш воситалари тармоқ сатҳида, операцион тизим сатҳида ва иловалар сатҳида ишлаши мумкин. Улар текширишлар сонини бора-бора кўпайтириш, ахборот тизимига "ичкарилаб бориш" ва унинг барча сатҳларини тадқиқлаш орқали заифликларни қидириши мумкин.

Тармоқ протоколлари ва сервислари ҳимояланишини таҳлиллаш воситалари. Ҳар қандай тармоқда абонентларнинг ўзаро алоқаси иккита ва ундан кўп узеллар орасида ахборот алмашиниш муолажаларини белгиловчи тармоқ протоколлари ва сервисларидан фойдаланишга асосланган. Тармоқ протоколлари ва сервисларини ишлаб чиқишда уларга ишланувчи ахборот хавфсизлигини таъминлаш бўйича талаблар (одатда шубхасиз етарли

бўлмаган) қўйилган. Шу сабабли, тармоқ протоколларида аниқланган заифликлар хусусида ахборотлар пайдо бўлмоқда. Натижада, корпоратив тармоқда фойдаланадиган барча протокол ва сервисларни доимо текшириш зарурияти туғилади.

Ҳимояланишни тахлиллаш тизими заифликларни аниқлаш бўйича тестлар сериясини бажаради. Бу тестлар нияти бузуқ одамларнинг корпоратив тармоқларга хужумларида қўлланиладиганига ўхшаш.

Заифликларни аниқлаш мақсадида сканерлаш текширувчи тизим хусусидаги дастлабки ахборотни, хусусан, рухсат этилган протоколлар ва очиқ портлар, операцион тизимнниг ишлатилувчи версиялари ва ҳ. хусусидаги ахборотни олиш билан бошланади. Сканерлаш кенг тарқалган хужумлар, масалан, тўлиқ саралаш усули бўйича паролларни танлашдан фойдаланиб, суқилиб киришни имитациялашга уриниш билан тугайди.

Ҳимояланишни тахлиллаш воситалари ёрдамида тармоқ сатҳида нафақат Internetнинг корпоратив тармоқдан рухсатсиз фойдаланиши имкониятини тестлаш, балки ташкилот ички тармоғида текширишни амалга ошириш мумкин. Тармоқ сатҳида ҳимояланишни тахлиллаш тизими ташкилот хавфсизлик даражасини баҳолашга ҳамда тармоқ дастурий ва аппарат таъминотини созлаш самарадорлигини назоратлашга хизмат қилади.

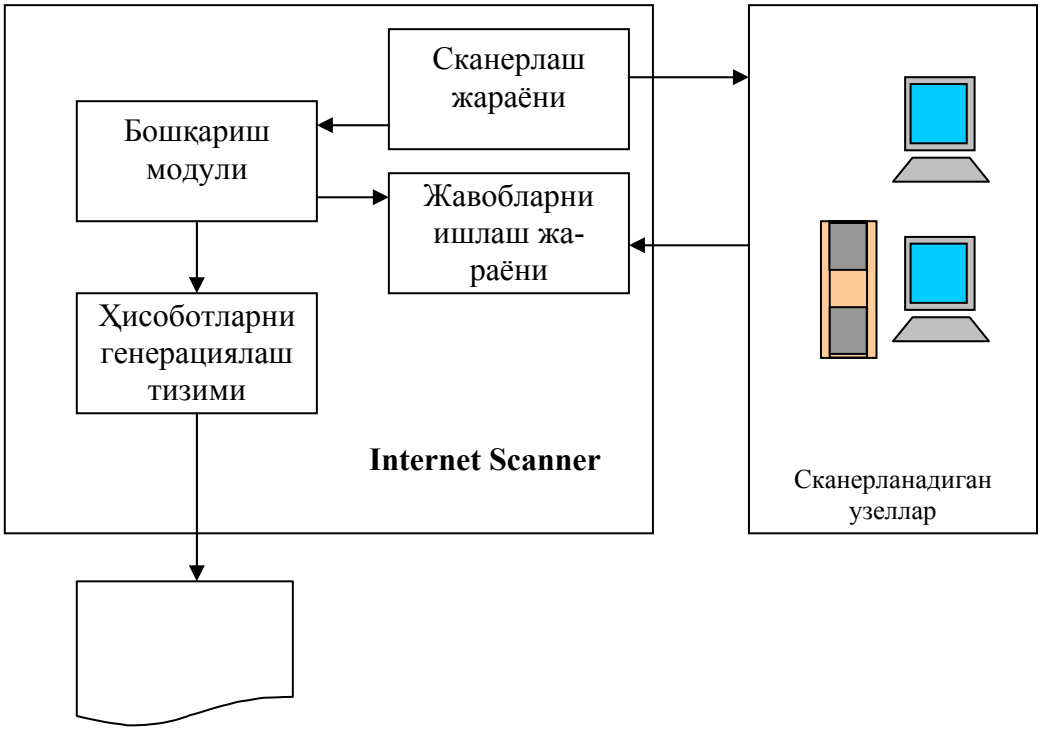
Ҳимояланишни тахлиллашни амалга оширувчи (Internet Scanner тизими мисолида) намунавий схема10.3-расмда келтирилган.

Ҳимояланишни тахлиллаш воситаларининг бу синфи нафақат тармоқ протоколлари ва сервислари, балки тармоқ билан ишлашга жавобгар тизимли ва татбиқий дастурий таъминоти заификларини ҳам тахлиллайди. Бундай таъминот қаторига Web-, FTP-, ва почта серверларини, тармоқлараро экранларни, браузерларни ва ҳ. киритиш мумкин.

Баъзи воситалар дастурий таъминотни тахлиллаш билан бир қаторда аппарат воситаларини сканерлайди. Бундай воситаларга коммутацияловчи ва маршрутловчи асбоб-ускуналар киради.

Операцион тизим ҳимояланишини тахлиллаш воситалари. Воситаларнинг бу синфи операцион тизим ҳимояланишига таъсир этувчи унинг

созланишларини текширишга аталган. Бундай созлашлар қуйидагиларни аниқлайди:



10.3–расм. Internet Scanner тизими мисолида ҳимояланганликни таҳлиллаш схемаси.

- фойдаланувчиларнинг ҳисоб ёзуви, масалан, парол узунлиги ва унинг таъсир муддати;

- фойдаланувчиларнинг жиддий тизимли файллардан фойдаланиш ҳуқуқлари;

- заиф тизимли файллар;

- ўрнатилган патчлар ва ҳ.

Операцион тизим сатҳидаги ҳимояланишни тахлиллаш тизимлари операцион тизимлар конфигурациясини назоратлашда ҳам ишлатилиши мумкин.

Тармоқ сатҳи ҳимояланишни тахлиллаш воситаларидан фарқли равишда, ушбу тизимлар тахлилланувчи тизимни ташқаридан эмас, балки ичкаридан сканерлайди, яъни улар ташқаридаги нияти бузуқ одамлар хужумларини имитацияламайди. Операцион тизим сатҳида ҳимояланишни тахлиллаш тизимларининг баъзилари (масалан, Internet Security Systems компаниясининг System Scanner тизими) заифликларни аниқлаш имконияти-

дан ташқари, аниқланган муаммоларнинг бир қисмини автоматик тарзда бартараф қилишга ёки ташкилотда қабул қилинган хавфсизлик сиёсатини қониқтирмайдиган тизим параметрларига тузатиш киритишга имкон беради.

Танланувчи ҳимоялашни тахлиллаш воситаларига қуйиладиган умумий талаблар. Танланувчи тизимга қўйиладиган мажбурий талаб-корхона тармоқ инфратузилмасини ўзгартириш заруриятининг йўқлиги. Акс ҳолда бундай қайтадан ташкил этишга қилинадиган харажат ҳимояланишни таҳлиллаш тизими нархидан ошиб кетиши мумкин. Ҳозирда бу талабга фақат Internet Security Systems компаниясининг Security Systems тизими жавоб беради.

Ҳимояланишни тахлиллаш воситаларини нотўғри ишлатиш улардан нияти бузуқ одамларнинг корпоратив тармоққа суқилиб кириш учун фойдаланишларига имкон яратади. Шу сабабли, ҳимояланишни тахлиллаш воситалари ўзларининг компонентларидан ва йиғилган маълумотлардан фойдаланишни чегараловчи механизмлар билан таъминланиши лозим. Бундай механизмларга қуйидагилар киради:

- фақат маъмур хуқуқига эга бўлган фойдаланувчи томонидан ушбу воситаларни ишга тушириш;

- сканерлаш маълумотлари архивини шифрлаш;

- масофадан бошқаришда уланишни аутентификациялаш;

- каталоглар билан ишлаш учун махсус хуқуқларни аниқлаш ва ҳ.

Заифликларни аниқлаш жараёнининг қуйидаги имкониятларига эътиборни қаратиш лозим:

- бир неча қурилма ёки сервисларни параллел ишлаш эвазига сканерлаш тезлигини ошириш;

- тизимдан рухсатсиз фойдаланишни олдини олиш учун ҳар бир сканерланувчи узелга билдириш қоғозини юбориш;

- ёлғон ишлашларни минималлаштириш учун тармоқни эксплуатация талабларига тўғрилаш.

Корпоратив тармоқ холатининг доимо ўзгариб туриши, унинг ҳимояланишига таъсир кўрсатади. Шу сабабли, ҳимояланишни тахлиллашнинг яхши тизими жадвал бўйича ишлаш режимига эга бўлиб, маъмур уни эслагунича ўзи тармоқ узеллари заифликларини текшириши ва пайдо

бўлган муаммолар хусусида нафақат маъмурни огоҳлантириши, балки аниқланган заифликларни йўқотиш усулларини тавсия этиши лозим.

Эътибор бериш зарур бўлган характеристикалардан бири- хисоботларни генерациялаш тизимининг мавжудлиги. Бу тизим фойдаланувчиларнинг турли категорияларлари – техник мутахассислардан тортиб то ташкилотлар раҳбарлари учун тафсилоти турли даражада бўлган хужжатларни яратишга имкон бериши лозим.

Хужжатларда маълумотларни ифодалаш шакли ҳам муҳим ҳисобланади. Фақат матнли ахборот билан тўлдирилган хужжатларнинг фойдаси бўлмайди. Графиклардан фойдаланиш эса маъмурга ташкилот тармоғидаги барча муаммоларни яққол намойиш этишга имкон беради. Ҳисоботларда аниқланган муаммоларни йўқотиш бўйича тавсияларнинг мавжудлиги ҳимояланишни тахлиллаш воситаларини танлашдаги мажбурий шарт ҳисобланади.

Доимо янги заифликларнинг аниқланиши ҳимояланишни тахлиллаш тизимининг заифликлар маълумотлари базасини тўлдира олиши имкониятига эга бўлишини тақозо этади. Бу заифликларни тавсифловчи махсус тил ёрдамида ёки тизим ишлаб чиқарувчилари томонидан заифликларни вақтивақти билан тўлдириш йўли билан амалга оширилади. Корпоратив тармоқ узелларининг ҳимояланиш даражасининг ўзгаришини тахлиллаш учун танланувчи восита ўтказилган сканерлаш сеанслари хусусидаги ахборотни тўпланишига имкон бериши лозим.

10.3. Хужумларни аниқлаш

Тармоқ ахборотини тахлиллаш усуллари. Моҳияти бўйича, хужумларни аниқлаш жараёни корпоратив тармоқда бўлаётган шубҳали ҳаракатларни баҳолаш жараёнидир. Бошқача айтганда хужумларни аниқлаш- ҳисоблаш ёки тармоқ ресурсларига йўналтирилган шубҳали ҳаракатларни идентификациялаш ва уларга реакция кўрсатиш жараёни. Ҳозирда хужумларни аниқлаш тизимида қуйидаги усуллар ишлатилади:

- статистик усул;

- эксперт тизимлари;
- нейрон тармоқлари.

Статистик усул. Статистик ёндашишнинг асосий афзаллиги – аллақачон ишлаб чиқилган ва ўзини танитган математик статистика аппаратини ишлатиш ва субъект характерига мослаш.

Аввал таҳлилланувчи тизимнинг барча субъектлари учун профиллар аниқланади. Ишлатиладиган профилларнинг эталондан ҳар қандай четланиши рухсат этилмаган фойдаланиш ҳисобланади. Статистик усуллар универсал ҳисобланади, чунки мумкин бўлган хужумларни ва улар фойдаланадиган заифликларни билиш талаб этилмайди. Аммо бу усуллардан фойдаланишда бир қанча муаммолар пайдо бўлади:

1. Статистик тизимлар ходисалар келиши тартибига сезувчанмаслар; баъзи холларда бир ходисанинг ўзи, келиши тартибига кўра аномал ёки нормал фаолиятни характерлаши мумкин.
2. Аномал фаолиятни адекват идентификациялаш мақсадида хужумларни аниқлаш тизими томонидан кузатилувчи характеристикалар учун чегаравий (бўсағавий) қийматларни бериш жуда қийин.
3. Статистик усуллар вақт ўтиши билан бузғунчилар томонидан шундай "ўрнатилиши" мумкинки, хужум ҳаракатлари нормал каби қабул қилинади.

Эксперт тизимлари. Эксперт тизими одам-эксперт билимларини қамраб олувчи қоидалар тўпламидан ташкил топган. Эксперт тизимидан фойдаланиш хужумларни аниқлашнинг кенг тарқалган усули бўлиб, хужумлар хусусидаги ахборот қоидалар кўринишида ифодаланади. Бу қоидалар ҳаракатлар кетма-кетлиги ёки сигнатуралар кўринишида ёзилиши мумкин. Бу қоидаларнинг ҳар бирининг бажарилишида рухсатсиз фаолият мавжудлиги хусусида қарор қабул қилинади. Бундай ёндашишнинг муҳим афзаллиги – ёлғон тревоганинг умуман бўлмаслиги.

Эксперт тизимининг маълумотлари базасида ҳозирда маълум бўлган аксарият хужумлар сценарияси бўлиши лозим. Эксперт тизимлари, дол-

зарбликни сақлаш мақсадида, маълумотлар базасини муттасил янгилашни талаб этади. Гарчи эксперт тизимлари қайдлаш журналларидаги маълумотларни кўздан кечиришга яхши имкониятни тавсия қилсада, сўралган янгиланиш эътиборсиз қолдирилиши ёки маъмур томонидан қўлда амалга оширилиши мумкин. Бу энг камида, эксперт тизими имкониятларининг бўшашига олиб келади.

Эксперт тизимларининг камчиликлари ичида энг асосийси – номаълум хужумларни акслантира олмаслиги. Бунда олдиндан маълум хужумнинг хатто озгина ўзгариши хужумларни аниқлаш тизимининг ишлашига жиддий тўсиқ бўлиши мумкин.

Нейрон тармоқлари. Хужумларни аниқлаш усулларининг аксарияти қоидалар ёки статистик ёндашиш асосида назоратланувчи муҳитни таҳлиллаш шаклларидан фойдаланади. Назоратланувчи муҳит сифатида қайдлаш журналлари ёки тармоқ трафиги кўрилиши мумкин. Бундай тахлиллаш маъмур ёки хужумларни яниқлаш тизими томонидан яратилган, олдиндан аниқланган қоидалар тўпламига таянади.

Хужумни вақт бўйича ёки бир неча нияти бузуқ одамлар ўртасида ҳар қандай бўлиниши эксперт тизимлар ёрдамида аниқлашга қийинчилик туғдиради. Хужумлар ва улар усулларининг турли-туманлиги туфайли, эксперт тизимлари қоидаларининг маълумотлар базасининг ҳатто доимий янгиланиши ҳам хужумлар диапазонини аниқ идентификациялашни кафолатламайди.

Нейрон тармоқларидан фойдаланиш эксперт тизимларининг юқорида келтирилган муаммоларни бартараф этишнинг бир усули ҳисобланади. Эксперт тизимлари фойдаланувчига кўрилаётган характеристикалар қоидалар маълумотлари базасидагига мос келиши ёки мос келмаслиги хусусида аниқ жавоб бераолса, нейротармоқ ахборотни тахлиллайди ва маълумотларни аниқлашга ўрганган характеристикаларига мос келишини баҳолаш имкониятини тақдим этади. Нейротармоқли ифодалашнинг мослик даражаси 100%га етиши мумкин, аммо танлаш хақиқийлиги тамоман қўйилган масала мисолларини тахлиллаш сифатига боғлиқ.

Аввал предмет соҳасининг олдиндан танлаб олинган мисолида нейротармоқни тўғри идентификациялашга "ўргатишади". Нейротармоқ реакцияси тахлилланади, қониқарли натижаларга эришиш мақсадида тизим созланади. Нейротармоқ ҳам вақт ўтиши билан, предмет соҳаси билан боғлиқ маълумотларни тахлиллашни ўтказишига қараб "тажриба орттиради".

Нейротармоқларнинг суиистеъмол қилинишни аниқлашдаги муҳим афзаллиги, уларнинг атайин қилинадиган хужумлар характеристикаларини "ўрганиш" ва тармоқда олдин кузатилганига ўхшамаган элементларни идентификациялаш қобилиятидир.

Юқорида тавсифланган хужумларни аниқлаш усулларининг ҳар бири афзалликларга ва камчиликларга эга. Шу сабабли, ҳозирда тавсифланган усулларнинг фақат биттасидан фойдаланувчи тизимни учратиш қийин. Одатда, бу усуллар биргаликда ишлатилади.

Хужумларни аниқлаш тизимларининг туркумланиши. Хужумларни аниқлаш тизимлари IDS(Intrusion Detection System)да ишлатилувчи хужумларни аниқловчи механизмлар бир неча умумий усулларга асосланган. Таъкидлаш лозимки, бу усуллар бир-бирини инкор этмайди. Аксарият тизимларда бир неча усулларнинг комбинациясидан фойдаланилади.

Хужумларни аниқлаш тизимлари қуйидаги аломатлари бўйича туркумланиши мумкин:

- реакция кўрсатиш усули бўйича;
- хужумларни фош этиш усули бўйича;
- хужум хусусидаги ахборотни йиғиш усули бўйича.

Реакция кўрсатиш усули бўйича пассив ва актив IDSлар фарқланади. Пассив IDS лар хужум фактларини қайдлайди, маълумотларни журнал файлига ёзади ва огоҳлантиришлар беради. Актив IDSлар, масалан, тармоқлараро экранни қайта конфигурациялаш ёки маршрутизатордан фойдаланиш руйхатини генерациялаш билан хужумга қарши ҳаракат қилишга уринади.

Хужумларни фош этиш усули бўйича IDSларни қуйидаги иккита категорияга ажратиш қабул қилинган:

- аномал ҳатти-ҳаракатни аниқлаш (anomaly-based);

- суиистеъмолликларни аниқлаш (misuse detection ёки signature-based).

Аномал ҳатти-ҳаракатни аниқлаш йўли билан хужумларни аниқлаш технологияси қуйидаги гипотезага асосланган. Фойдаланувчининг аномал ҳатти-ҳаракати (яъни хужуми ёки қандайдир ғаразли ҳаракати) – нормал ҳатти-ҳаракатдан четлашиш. Аномал ҳатти-ҳаракатга мисол тариқасида қисқа вақт оралиғида уланишларнинг катта сонини, марказий процессорнинг юқори юкланишини ва ҳ. кўрсатиш мумкин.

Агар фойдаланувчининг нормал ҳатти-ҳаракати профилини бир маънода тавсифлаш мумкин бўлганида, ҳар қандай ундан четланишларни аномал ҳатти-ҳаракат сифатида идентифкациялаш мумкин бўлар эди. Аммо, аномал ҳатти-ҳаракат ҳар доим ҳам хужум бўлавермайди. Масалан, тармоқ маъмури томонидан юборилган кўп сонли сўровларни хужумларни аниқлаш тизими "хизмат кўрсатишдан воз кечиш" хилидаги хужум сифатида идентификациялаши мумкин.

Ушбу технология асосидаги тизимдан фойдаланилганда иккита кескин ҳолат юз бериши мумкин:

- хужум бўлмаган аномал ҳатти-ҳаракатни аниқлаш ва уни хужумлар синфига киритиш;

- аномал ҳатти-ҳаракат таърифига мос келмайдиган хужумларни ўтказиб юбориш. Бу ҳолат хужум бўлмаган аномал ҳатти ҳаракатни хужумлар синфига киритишга нисбатан хавфлироқ ҳисобланади.

Бу категория тизимларини созлашда ва эксплуатациясида маъмур қуйидаги қийинчиликларга дуч келади:

- фойдаланувчи профилини қуриш сермеҳнат масала бўлиб, маъмурдан катта дастлабки ишларни талаб этади.

- юқорида келтирилган иккита кескин ҳаракатлардан бирининг пайдо бўлиши эҳтимоллигини пасайтириш учун фойдаланувчи ҳатти-ҳаракатининг чегаравий қийматларини аниқлаш зарур.

Аномал ҳатти-ҳаракатларни аниқлаш технологияси хужумларнинг янги хилини аниқлашга мўлжалланган. Унинг кимчилиги - доимо "ўрганиш" зарурияти.

Суиистеъмолликларни аниқлаш йўли билан хужумларни аниқлаш технологиясининг моҳияти хужумларни сигнатура кўринишида тавсифлаш ва ушбу сигнатурани назоратланувчи маконда (тармоқ трафигида ёки қайдлаш журналида) қидиришдан иборат. Хужум сигнатураси сифатида аномал фаолиятни характерловчи ҳаракатлар шаблони ёки символлар сатри ишлатилиши мумкин. Бу сигнатуралар вирусга қарши тизимларда ишлатилувчи маълумотлар базасига ўхшаш маълумотлар базасида сақланади. Таъкидлаш лозимки, вирусга қарши резидент мониторлар хужумларни аниқлаш тизимларининг хусусий холи ҳисобланади. Аммо бу йўналишлар бошидан параллел ривожланганлари сабабли, уларни ажратиш қабул қилинган. Ушбу хил тизимлар барча маълум хужумларни аниқласада, янги, ҳали маълум бўлмаган хужумларни аниқлай олмайди.

Бу тизимларни эксплуатациясида ҳам маъмурларга муаммоларни дуч келади. Биринчи муаммо - сигнатураларни тавсифлаш механизмларини, яъни хужумларни тавсифловчи тилларни яратиш. Иккинчи муаммо, биринчи муаммо билан боғлиқ бўлиб, хужумларни шундай тавсифлаш лозимки, унинг барча модификацияларини қайдлаш имкони туғилсин.

Хужум хусусидаги ахборотни йиғиш усули бўйича туркумлаш энг оммавий ҳисобланади:

- тармоқ сатҳида хужумларни аниқлаш (network-based);
- хост сатҳида хужумларни аниқлаш (host-based);
- илова сатҳида хужумларни аниқлаш (application-based).

Тармоқ сатҳида хужумларни аниқлаш тизимида тармоқдаги трафикни эшитиш орқали нияти бузуқ одамларнинг мумкин бўлган ҳаракатлари аниқланади. Хужумни қидириш "хостдан-хостгача" принципи бўйича амалга оширилади. Ушбу хилга тааллуқли тизимлар, одатда хужумлар сигнатурасидан ва "бир зумда" тахлиллашдан фойдаланиб, тармоқ трафигини тахлиллайди. "Бир зумда" тахлиллаш усулига биноан тармоқ трафиги реал ёки унга яқинроқ вақтда мониторингланади ва мос аниқлаш алгоритмларидан

фойдаланилади. Кўпинча рухсатсиз фойдаланиш фаолиятини характерловчи трафикдаги маълум сатрларни қидириш механизмларидан фойдаланилади.

Хост сатҳида хужумларни аниқлаш тизими маълум хостда нияти бузуқ одамларни мониторинглаш, детектирлаш ва ҳаракатларига реакция кўрсатишга аталган. Тизим ҳимояланган хостда жойлашиб, унга қарши йўналтирилган ҳаракатларни текширади ва ошкор қилади. Бу тизимлар операцион тизим ёки иловаларнинг қайдлаш журналларини тахлиллайди. Қайдлаш журналларини тахлиллаш усулини амалга ошириш осон бўлсада, у қуйидаги камчиликларга эга:

- журналда қайд этилувчи маълумотлар ҳажмининг катталиги назоратланувчи тизим ишлаши тезлигига салбий таъсир кўрсатади;

- қайдлаш журналини тахлиллашни мутахассислар ёрдамисиз амалга ошириб бўлмайди;

- ҳозиргача журналларни сақлашнинг унификацияланган формати мавжуд эмас;

- қайдлаш журналларидаги ёзувни тахлиллаш реал вақтда амалга оширилмайди.

IDSнинг учинчи хили маълум иловадаги муаммоларни қидиришга асосланган.

Хужумларни аниқлаш тизимининг компонентлари ва архитектураси. Мавжуд ечимларнинг тахлили хужумларни аниқлашнинг намунавий тизими компонентларининг рўйхатини келтиришга имкон беради.

Кузатиш модули назоратланувчи макондан (қайдлаш журнали ёки тармоқ трафиги) маълумотларни йиғишни таъминлайди. Унинг қуйидаги номлари ҳам учрайди: сенсор (sensor), монитор (monitor), зонд(probe) ва ҳ. Хужумларни аниқлаш тизими архитектурасининг қурилишига боғлиқ ҳолда кузатиш модули бошқа компонентлардан алоҳида, бошқа компьютерда жойлашиши мумкин.

Хужумларни аниқлаш қисм тизими асосий модул бўлиб, кузатиш модулидан олинадиган ахборотни тахлиллайди. Ушбу тахлиллаш натижаси бўйича қисм тизим хужумларни идентификациялаш, реакция кўрсатиш ва-

риантлари бўйича тўхтамга келиши, маълумотлар омборида хужумлар хусусидаги ахборотни сақлаши мумкин ва ҳ.

Билимлар базасида, хужумларни аниқлаш тизимларида ишлатиладиган усулларга боғлиқ ҳолда, фойдаланувчилар ва ҳисоблаш тизим профиллари, рухсатсиз фойдаланишларни характерловчи хужум сигнатуралари ёки шубхали сатрлар сақланиши мумкин. Билимлар базаси хужумларни аниқлаш тизимларини ишлаб чиқарувчилари, тизимдан фойдаланувчилар ёки учинчи томон, масалан бу тизимни мададловчи аутсорсинг компанияси томонидан тўлдирилиши мумкин.

Маълумотлар омбори хужумларни аниқлаш тизими ишлаши жараёнида йиғилган маълумотларнинг сақланишини таъминлайди.

График интерфейс тизимнинг ниҳоятда зарурий компоненти бўлиб, хужумларни аниқлаш тизими ишлашини бошқарувчи операцион тизимга боғлиқ ҳолда де-факто Windows ва Unix стандартларига мос келиши лозим.

Реакция кўрсатиш қисм тизими аниқланган хужумлар ва бошқа назоратланувчи ходисаларга реакция кўрсатишни амалга оширади. Мавжуд тизимларда ишлатиладиган реакция кўрсатиш усулларини қуйидаги учта категорияга ажратиш мумкин:

- билдириш;
- сақлаш;
- фаол реакция кўрсатиш.

Билдириш усули бўйича хужум хусусидаги ахборот хавфсизлик маъмурига тизимнинг консолига ёки электрон почта бўйича, пейджерга факс ёки телефон орқали жўнатилиши мумкин.

Сақлаш усулига реакция кўрсатишнинг қуйидаги вариантлари тааллуқли:

- ходисаларни маълумотлар базасида қайдлаш;
- хужумларни реал вақт масштабида тиклаш.

Биринчи вариант ҳимоялашнинг бошқа тизимларида ҳам кенг қўлланилади. Иккинчи вариантни амалга ошириш учун хужум қилувчини компания тармоғига ўтказиб юбориш ва унинг барча ҳаракатларини қайдлаш лозим. Бу хавфсизлик маъмурига кейин вақтнинг реал масштабида

(ёки берилган тезликда) хужум қилувчи томонидан қилинган барча ҳаракатларни тиклашга, муваффақиятли тахлиллашга ва уларни кейинчалик бартараф этишга ҳамда муҳокама қилиш жараёнида йиғилган ахборотдан фойдаланишга имкон беради.

Фаол реакция кўрсатиш категориясига қуйидаги вариантлар тааллуқли:

- хужум қилувчи ишини блокировка қилиш;
- хужум қилунувчи узел билан сеансни тугаллаш;
- тармоқ асбоб-ускуналари ва ҳимоя воситаларини бошқариш.

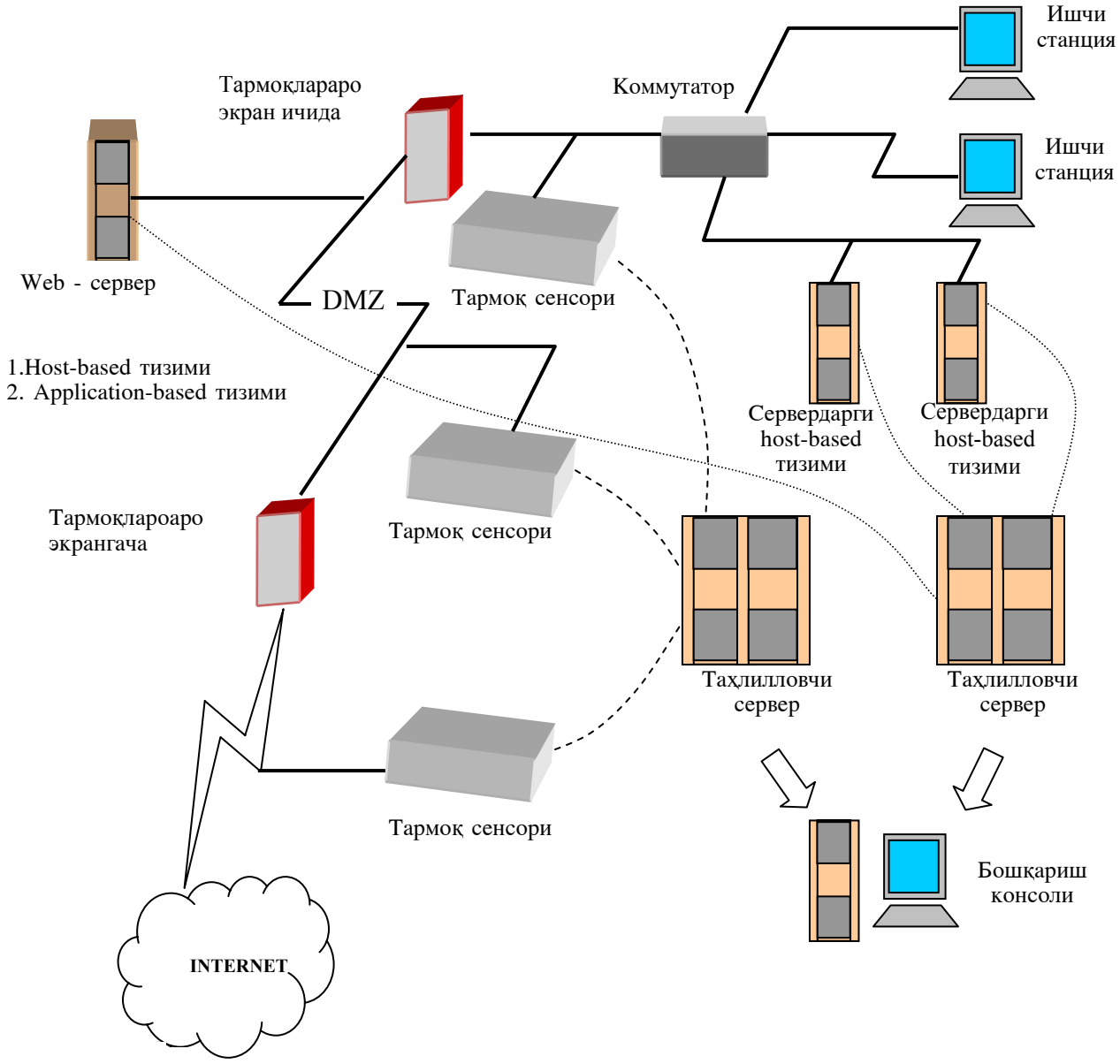
Реакция кўрсатиш механизмларининг ушбу категорияси бир томондан етарлича самарали бўлса, иккинчи томондан улардан жуда эҳтиётлик билан фойдаланиш зарур, чунки уларни нотўғри ишлатиш бутун корпоратив ахборот тизими ишга лаёқатлигининг бузилишига олиб келиши мумкин.

Компонентларни бошқариш қисм тизими хужумларни аниқлаш тизимининг турли компонентларини бошқаришга аталган. "Бошқариш" атамаси орқали хужумларни аниқлаш тизимининг турли компонентлари (масалан кузатиш модуллари) учун хавфсизлик сиёсатини ўзгартириш, ҳамда ушбу компонентлардан ахборотни (масалан, қайдланган хужум хусусидаги) олиш тушунилади. Бошқариш ички протоколлар ва интерфейслар ва ишлаб чиқилган стандартлар (масалан, SNMP) ёрдамида амалга оширилиши мумкин.

Хужумларни аниқлаш тизимлари иккита архитектура – "автоном агент" ва "агент-менеджер" архитектуралари асосида қурилади. Биринчи ҳолда тармоқнинг ҳар бир ҳимояланувчи узел ва сегментларига тизим агентлари ўрнатилиб, бу агентлар ўзаро ахборот алмаша олмайдилар, ҳамда уларни ягона консол орқали марказлаштирилган ҳолда бошқариб бўлмайди. "Агент-менеджер" архитектураси бу камчиликлардан холи. Бу ҳолда катта тармоқнинг турли қисмларида жойлашган кўпгина IDSдан иборат хужумларни аниқлашнинг тақсимланган тизими dIDS (distributed IDS)да маълумотларни йиғиш серверлари ва марказий тахлилловчи сервер қайдланувчи маълумотларни марказлаштирилган йиғишни ва тахлиллашни амалга оширади. dIDS модулларини бошқариш бошқаришнинг марказий консоли

орқали амалга оширади. Филиаллари турли худудлар, ҳатто шахарлар бўйича тарқалган йирик ташкилотлар учун бундай архитектуранинг ишлатилиши жиддий аҳамиятга эга.

dIDS ишлашининг умумий схемаси 10.4-расмда келтирилган.



10.4-расм. Тақсимланган IDS ишлашининг умумий схемаси

Бундай тизим турли IDSлардан хужумлар хусусидаги ахборотларни марказлаштирилиши эвазига корпоратив қисм тармоқ ҳимояланишини кучайтиришга имкон беради. Хужумларни аниқловчи тақсимланган тизим dIDS қуйидаги қисм тизимлардан ташкил топган: бошқариш консоли, таҳлилловчи серверлар, тармоқ агентлари, хужум хусусидаги ахборотни йиғувчи сервер. Марказий таҳлилловчи сервер одатда маълумотлар базаси

ва Web-сервердан ташкил топган бўлиб, хужумлар хусусидаги ахборотни сақлашга ва қулай Web-интерфейс ёрдамида маълумотларни манипуляция-лашга имкон беради. Тармоқ агенти dIDSнинг энг муҳим компонентларидан бири ҳисобланиб, мақсади марказий тахлилловчи серверга хужум хусусида хабар бериш бўлган кичкина дастурдир. Хужум хусусидаги ахборотни йиғувчи сервер марказий тахлилловчи серверга мантиқий таянган ва тармоқ агентларидан олинган маълумотларни гуруҳлашда фойдаланиладиган пара-метрларни белгилайди.

Маълумотларни гурухлашни қуйидаги параметрлар бўйича амалга ошириш мумкин:

- хужум қилувчининг IP-адреси;
- қабул қилувчининг порти;
- агент номери;
- сана, вақт;
- протокол;
- хужум хиллари ва ҳ.

IDSдан фойдаланиш самарадорлигига қандайдир шубхалар бўлишига қарамай, фойдаланувчилар IDSнинг очиқ тарқатилувчи ва тижорат воситаларидан кенг фойдаланадилар.

10.4. Компьютер вируслари ва вирусдан ҳимояланиш муаммолари

Компьютер вирусининг кўп таърифлари мавжуд. Биринчи таърифни 1984 йили Фред Коэн берган: "Компьютер вируси – бошқа дастурларни, уларга ўзини ёки ўзгартирилган нусхасини киритиш орқали, уларни моди-фикациялаш билан заҳарловчи дастур. Бунда киритилган дастур кейинги кўпайиш қобилиятини сақлайди". Вируснинг ўз-ўзидан кўпайиши ва ҳисоблаш жараёнини модификациялаш қобилияти бу таърифдаги таянч ту-шунчалар ҳисобланади. Компьютер вирусининг ушбу хусусиятлари тирик табиат организмларида биологик вирусларнинг паразитланишига ўҳшаш.

Ҳозирда компьютер вируси деганда қуйидаги хусусиятларга эга бўлган дастурий код тушунилади:

- аслига мос келиши шарт бўлмаган, аммо аслининг хусусиятларига (ўз-ўзини тиклаш) эга бўлган нусхаларни яратиш қобилияти;

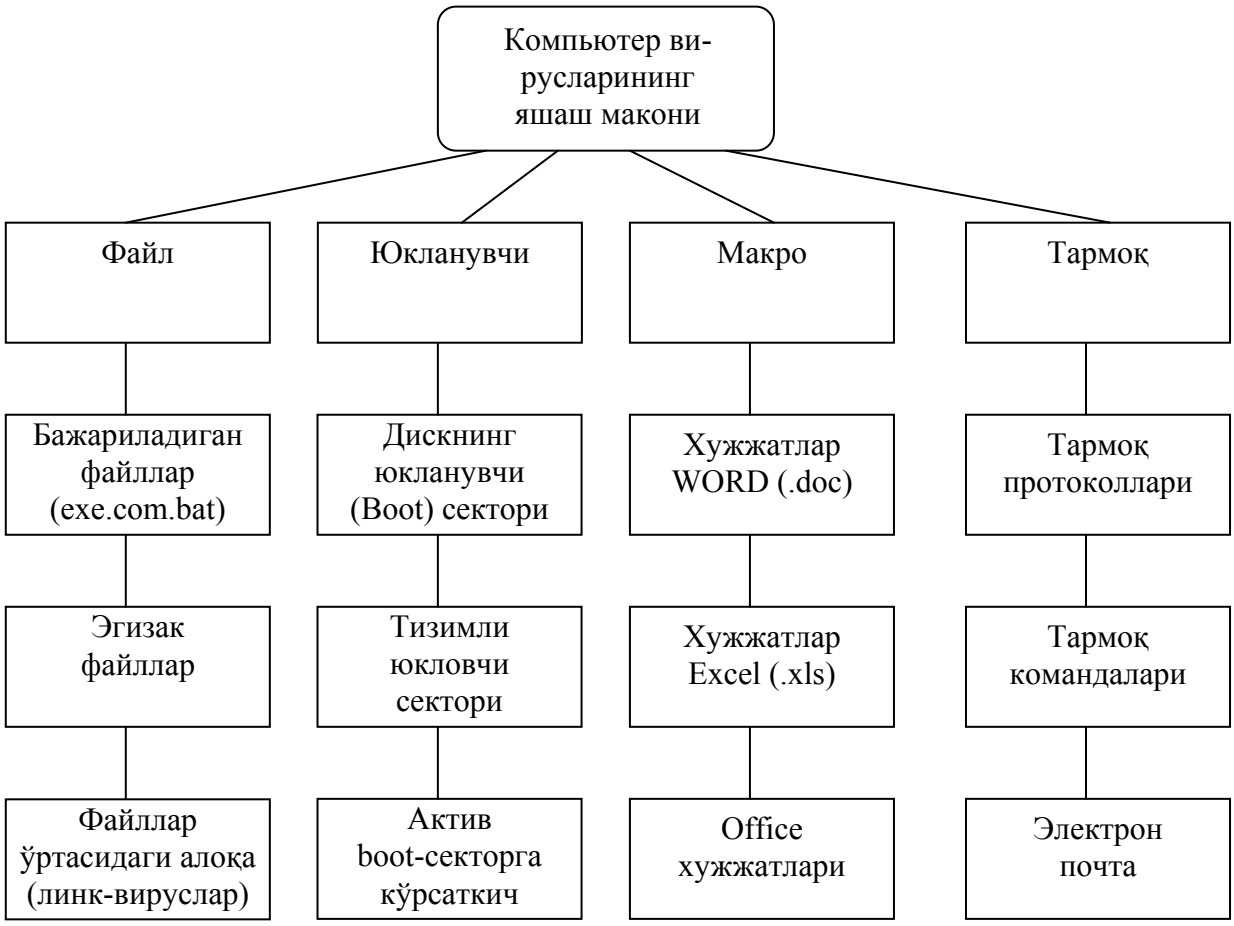
- ҳисоблаш тизимининг бажарилувчи объектларига яратилувчи нусхаларнинг киритилишини таъминловчи механизмларнинг мавжудлиги.

Таъкидлаш лозимки, бу хусусиятлар зарурий, аммо етарли эмас. Кўрсатилган хусусиятларни ҳисоблаш муҳитидаги зарар келтирувчи дастур таъсирининг деструктивлик ва сир бой бермаслик хусусиятлари билан тўлдириш лозим.

Вирусларни қуйидаги асосий аломатлари бўйича туркумлаш мумкин:

- яшаш макони;
- операцион тизим;
- ишлаш алгоритми хусусияти;
- деструктив имкониятлари.

Компьютер вирусларини яшаш макони, бошқача айтганда вируслар киритилувчи компьютер тизими объектларининг хили бўйича туркумлаш асосий ва кенг тарқалган туркумлаш ҳисобланади (10.5-расм).



10.5-расм. Яшаш макони бўйича компьютер вирусларининг туркумланиши.

Файл вируслари бажарилувчи файлларга турли усуллар билан киритилади (энг кўп тарқалган вируслар хили), ёки файл-йўлдошларни (компаньон вируслар) яратади ёки файлли тизимларни (link-вируслар) ташкил этиш хусусиятидан фойдаланади.

Юклама вируслар ўзини дискнинг юклама секторига (boot - секторига) ёки винчестернинг тизимли юкловчиси (Master Boot Record) бўлган секторга ёзади. Юклама вируслар тизим юкланишида бошқаришни олувчи дастур коди вазифасини бажаради.

Макровируслар ахборотни ишловчи замонавий тизимларнинг макродастурларини ва файлларини, хусусан MicroSoft Word, MicroSoft Excel ва ҳ. каби оммавий муҳаррирларнинг файл-хужжатларини ва электрон жадвалларини заҳарлайди.

Тармоқ вируслари ўзини тарқатишда компьютер тармоқлари ва электрон почта протоколлари ва командаларидан фойдаланади. Баъзида тармоқ вирусларини "қурт" хилидаги дастурлар деб юритишади. Тармоқ вируслари Internet-қуртларга (Internet бўйича тарқалади), IRC-қуртларга (чатлар, Internet Relay Chat) бўлинади.

Компьютер вирусларининг кўпгина комбинацияланган хиллари ҳам мавжуд, масалан – тармоқли макровирус таҳрирланувчи хужжатларни захарлайди, ҳамда ўзининг нусхаларини электрон почта орқали тарқатади. Бошқа бир мисол сифатида файл-юклама вирусларини кўрсатиш мумкинки, улар файлларни ҳамда дискларнинг юкланадиган секторини заҳарлайди.

Вирусларнинг ҳаёт даври. Ҳар қандай дастурдагидек компьютер вируслари ҳаёт даврининг иккита асосий босқичини сақланиш ва бажарилиш босқичларини ажратиш мумкин.

Сақланиш босқичи вируснинг дискда у киритилган объект билан биргаликда шундайгина сақланиш даврига тўғри келади. Бу босқичда вирус вирусга қарши дастур таъминотига заиф бўлади, чунки у фаол эмас ва ҳимояланиш учун операцион тизимни назорат қила олмайди.

Компьютер вирусларининг *бажарилиш даври*, одатда, бешта босқични ўз ичига олади:

1. Вирусни хотирага юклаш.

2. Қурбонни қидириш.
3. Топилган қурбонни заҳарлаш.
4. Деструктив функцияларни бажариш.
5. Бошқаришни вирус дастур-элтувчисига ўтказиш.

Вирусни хотирага юклаш. Вирусни хотирага юклаш операцион тизим ёрдамида вирус киритилган бажарилувчи объект билан бир вақтда амалга оширилади. Масалан, агар фойдаланувчи вирус бўлган дастурий файлни ишга туширса, равшанки, вирус коди ушбу файл қисми сифатида хотирага юкланади. Оддий ҳолда, вирусни юклаш жараёни-дискдан оператив хотирага нусхалаш бўлиб, сўнгра бошқариш вирус бадани кодига узатилади. Бу ҳаракатлар операцион тизим томонидан бажарилади, вируснинг ўзи пассив ҳолатда бўлади. Мураккаброқ вазифаларда вирус бошқаришни олганидан сўнг ўзининг ишлаши учун қўшимча ҳаракатлар бажариши мумкин. Бу билан боғлиқ иккита жиҳат кўрилади.

Биринчиси вирусларни аниқлаш муолажасининг максимал мураккаблашиши билан боғлиқ. Сақланиш босқичида баъзи вируслар ҳимояланишни таъминлаш мақсадида етарлича мураккаб алгоритмдан фойдаланади. Бундай мураккаблашишга вирус асосий баданини шифрлашни киритиш мумкин. Аммо фақат шифрлашни ишлатиш чала чора ҳисобланади, чунки юкланиш босқичида расшифровкани таъминловчи вирус қисми очиқ кўринишда сақланиши лозим. Бундай ҳолатдан қутилиш учун вирусларни ишлаб чиқувчилар расшифровка қилувчи кодини "мутациялаш" механизмидан фойдаланади. Бу усулнинг моҳияти шундан иборатки, объектга вирус нусхаси киритилишида унинг расшифровка қилувчига тааллуқли қисми шундай модификацияланадики, оригинал билан матнли фарқланиш пайдо бўлади, аммо иш натижаси ўзгармайди.

Кодни мутациялаш механизмидан фойдаланувчи вируслар *полиморф вируслар* номини олган. Полифморф вируслар (polymorphic)-қийин аниқланадиган вируслар бўлиб, сигнатураларга эга эмас, яъни таркибида бирорта ҳам кодининг доимий қисми йўқ. Полиморфизм файлли, юкламали ва макровирусларда учрайди.

Стелс-алгоритмлардан фойдаланилганда вируслар ўзларини тизимда тўла ёки қисман беркитишлари мумкин. стелс-алгоритмларидан фойдаланадиган вируслар – *стелс-вируслар* (Stealth) деб юритилади. Стелс вируслар операцион тизимнинг шикастланган файлларга мурожаатини ушлаб қолиш йўли билан ўзини яшаш маконидалигини яширади ва операцион тизимни ахборотни шикастланмаган қисмига йўналтиради.

Иккинчи жиҳат *резидент вируслар* деб аталувчи вируслар билан боғлиқ. Вирус ва у киритилган объект операцион тизим учун бир бутун бўлганлиги сабабли, юкланишдан сўнг улар, табиий, ягона адрес маконида жойлашади. Объект иши тугаганидан сўнг у оператив хотирадан бўшалади. Бунда бир вақтнинг ўзида вирус ҳам бўшалиб сақланишнинг пассив босқичига ўтади. Аммо баъзи вируслар хили хотирада сақланиш ва вирус элтувчи иши тугашидан сўнг фаол қолиш қобилиятига эга. Бундай вируслар резидент номини олган. Резидент вируслар, одатда, фақат операцион тизимга рухсат этилган имтиёзли режимлардан фойдаланиб яшаш маконини заҳарлайди ва маълум шароитларда зараркунандалик вазифасини бажаради. Резидент вируслар хотирада жойлашади ва компьютер ўчирилишигача ёки операцион тизим қайта юкланишигача фаол ҳолда бўлади.

Резидент бўлмаган вируслар фақат фаоллашган вақтларида хотирага тушиб заҳарлаш ва заракунандалик вазифаларини бажаради. Кейин бу вируслар хотирани бутунлай тарк этиб яшаш маконида қолади.

Таъкидлаш лозимки, вирусларни резидент ва резидент бўлмаганларга ажратиш фақат файл вирусларига тааллуқли. Юкланучи ва макровируслар-резидент вирусларга тегишли.

Қурбонни қидириш. Қурбонни қидириш усули бўйича вируслар иккита синфга бўлинади. Биринчи синфга операцион тизим функцияларидан фойдаланиб фаол қидиришни амалга оширувчи вируслар киради. Иккинчи синфга қидиришнинг пассив механизмларини амалга оширувчи, яъни дастурий файлларга тузоқ қўювчи вируслар тааллуқли.

Топилган қурбонни заҳарлаш. Оддий ҳолда заҳарлаш деганда қурбон сифатида танланган объектда вирус кодининг ўз-ўзини нусхалаши тушунилади.

Аввал файл вирусларининг заҳарлаш хусусиятларини кўрайлик. Бунда иккита синф вируслари фарқланади. Биринчи синф вируслари ўзининг кодини дастурий файлга бевосита киритмайди, балки файл номини ўзгартириб, вирус бадани бўлган янги файлни яратади. Иккинчи синфга қурбон файлларига бевосита кирувчи вируслар тааллуқли. Бу вируслар киритилиш жойлари билан характерланади. Қуйидаги вариантлар бўлиши мумкин:

1. ***Файл бошига киритиш.*** Ушбу усул MS-DOSнинг *com*-файллари учун энг қулай ҳисобланади, чунки ушбу форматда хизматчяи сарлавҳалар кўзда тутилган.
2. ***Файл охирига киритиш.*** Бу усул энг кўп тарқалган бўлиб, вируслар кодига бошқаришни узатиш дастурнинг биринчи командаси (*com*) ёки файл сарлавҳасини (*exe*) модификациялаш орқали таъминланади.
3. ***Файл ўртасига киритиш.*** Одатда бу усулдан вируслар тузилмаси олдиндан маълум файлларга (масалан, *Command.com* файли) ёки таркибида бир хил қийматли байтлар кетма-кетлиги бўлган, узунлиги вирус жойлашишига етарли файлларга татбиқан фойдаланади.

Юклама вируслар учун заҳарлаш босқичининг хусусиятлари улар киритилувчи объектлар – қайишқоқ ва қаттиқ дискларнинг юкланиш секторларининг сифати ва қаттиқ дискнинг бош юклама ёзуви (MBR) орқали аниқланади. Асосий муаммо-ушбу объект ўлчамларининг чегараланганлиги. Шу сабабли, вируслар ўзларининг қурбон жойида сиғмаган қисмини дискда сақлаши, ҳамда заҳарланган юкловчи оригинал кодини ташиши лозим.

Макровируслар учун заҳарлаш жараёни танланган хужжат-қурбонда вирус кодини сақлашдан иборат. Баъзи ахборотни ишлаш дастурлари учун буни амалга ошириш осон эмас, чунки хужжат файллари форматининг макропрограммаларни сақлаши кўзда тутилмаган бўлиши мумкин.

Деструктив функцияларни бажариш. Деструктив имкониятлари бўйича безиён, хавфсиз, хавфли ва жуда хавфли вируслар фарқланади.

Безиён вируслар - ўз-ўзидан тарқалиш механизми амалга оширилувчи вируслар. Улар тизимга зарар келтирмайди, фақат дискдаги бўш хотирани сарфлайди холос.

Хавфсиз вируслар – тизимда мавжудлиги турли таассурот (овоз, видео) билан боғлиқ вируслар, бўш хотирани камайтирсада, дастур ва маълумотларга зиён етказмайди.

Хавфли вируслар – компьютер ишлашида жиддий нуқсонларга сабаб бўлувчи вируслар. Натижада дастур ва маълумотлар бузилиши мумкин.

Жуда хавфли вируслар – дастур ва маълумотларни бузилишига ҳамда компьютер ишлашига зарур ахборотни ўчирилишига бевосита олиб келувчи, муолажалари олдиндан ишлаш алгоритмларига жойланган вируслар.

Бошқаришни вирус дастур – элтувчисига ўтказиш. Таъкидлаш лозимки, вируслар бузувчилар ва бузмайдиганларга бўлинади.

Бузувчи вируслар дастурлар заҳарланганида уларнинг ишга лаёқатлигини сақлаш хусусида қайғурмайдилар, шу сабабли уларга ушбу босқичнинг маъноси йўқ.

Бузмайдиган вируслар учун ушбу босқич хотирада дастурни коррект ишланиши шарт бўлган кўринишда тиклаш ва бошқаришни вирус дастур-элтувчисига ўтқазиш билан боғлиқ.

Зарар келтирувчи дастурларнинг бошқа хиллари. Вируслардан ташқари зарар келтирувчи дастурларнинг қуйидаги хиллари мавжуд:

- троян дастурлари;

- мантиқий бомбалар;

- масофадаги компьютерларни яширинча маъмурловчи хакер утилиталари;

- Internetдан ва бошқа конфиденциал ахборотдан фойдаланиш паролларини ўғирловчи дастурлар.

Улар орасида аниқ чегара йўқ: троян дастурлари таркибида вируслар бўлиши, вирусларга мантиқий бомбалар жойлаштирилиши мумкин ва ҳ.

Троян дастурлар ўзлари кўпаймайди ва тарқатилмайди. Ташқаридан троян дастурлар мутлақо беозор кўринади, ҳатто фойдали функцияларни тавсия этади. аммо фойдаланувчи бундай дастурни компьютерига юклаб,

ишга туширса, дастур билдирмай зарар келтирувчи функцияларни бажариши мумкин. Кўпинча троян дастурлар вирусларни дастлабки тарқатишда, Internet орқали масофадаги компьютердан фойдаланишда, маълумотларни ўғирлашда ёки уларни йўқ қилишда ишлатилади.

Мантиқий бомба – маълум шароитларда зарар келтирувчи ҳаракатларни бажарувчи дастур ёки унинг алоҳида модуллари. Мантиқий бомба, масалан, маълум сана келганда ёки маълумотлар базасида ёзув пайдо бўлганида ёки йўқ бўлганида ва ҳ. ишга тушиши мумкин. Бундай бомба вирусларга, троян дастурларга ва оддий дастурларга жойлаштирилиши мумкин.

Вируслар ва зарар келтирувчи дастурларни тарқатиш каналлари. Компьютерлар ва корпоратив тармоқларни ҳимояловчи самарадор тизимни яратиш учун қаердан хавф туғилишини аниқ тасаввур этиш лозим. Вируслар тарқалишнинг жуда хилма-хил каналларини топади. Бунинг устига эски усулларга янгиси қўшилади.

Тарқатишнинг классик (мумтоз) усуллари. Файл вируслари дастур файллари билан биргаликда дискетлар ва дастурлар алмашишда, тармоқ катологларидан, Web- ёки FTP – серверлардан дастурлар юкланишида тарқатилади. Юклама вируслар компьютерга фойдаланувчи заҳарланган дискетани дисководда қолдириб, сўнгра операцион тизимни қайта юклашида тушиб қолади. Юклама вирус компьютерга вирусларнинг бошқа хили орқали киритилиши мумкин. Макрокоманда вируслари MicroSoft Word, Excel, Access файллари каби офис хужжатларининг захарланган файллари алмашинишида тарқалади.

Агар заҳарланган компьютер локал тармоққа уланган бўлса вирус осонгина файл-сервер дискларига тушиб қолиши, у ердан каталоглар орқали тармоқнинг барча компьютерларига ўтиши мумкин. Шу тариқа вирус эпидемияси бошланади. Вирус тармоқда шу вирус тушиб қолган компьютер фойдаланувчиси хуқуқлари каби хуқуққа эга эканлигини тизим маъмури унутмаслиги лозим. Шунинг учун у фойдаланувчи фойдаланадиган барча каталогларга тушиб қолиши мумкин. Агар вирус тармоқ маъмури ишчи станциясига тушиб қолса оқибати жуда оғир бўлиши мумкин.

Электрон почта.

Ҳозирда Internet глобал тармоғи вирусларнинг асосий манбаи ҳисобланади. Вируслар билан заҳарланишларнинг аксарияти MicroSoft Word форматида хатлар алмашишда содир бўлади. Электрон почта макрокоманда вирусларини тарқатиш канали вазифасини ўтайди, чунки ахборотлар билан бир қаторда кўпинча офис хужжатлари жўнатилади.

Вируслар билан заҳарлаш билмасдан ва ёмон ниятда амалга оширилиши мумкин. Масалан, макровирус билан заҳарланган муҳарриридан фойдаланувчи ўзи шубҳа қилмаган ҳолда, адресатларга заҳарланган хатларни жўнатиши мумкин. Иккинчи тарафдан нияти бузуқ одам атайин электрон почта орқали ҳарқандай хавфли дастурий кодни жўнатиши мумкин.

Троян Web-сайтлар. Фойдаланувчилар вирусни ёки троян дастурни Internet сайтларининг оддий кузатишда, троян Web-сайтни кўрганида олиши мумкин. Фойдаланувчи браузерларидаги хатоликлар кўпинча троян Web-сайтлари фаол компонентларининг фойдаланувчи компьютерларига зарар келтирувчи дастурларни киритишига сабаб бўлади. Троян сайтни кўришга таклифни фойдаланувчи оддий электрон хат орқали олиши мумкин.

Локал тармоқлар.

Локал тармоқлар ҳам тезликда заҳарланиш воситаси ҳисобланади. Агар ҳимоянинг зарурий чоралари кўрилмаса, заҳарланган ишчи станция локал тармоққа киришда сервердаги бир ёки бир неча хизматчи файлларни заҳарлайди. Бундай файллар сифатида Login.com хизматчи файлни, фирмада қўлланилувчи Excel-жадваллар ва стандарт хужжат-шаблонларни кўрсатиш мумкин. Фойдаланувчилар бу тармоққа киришида сервердан заҳарланган файлларни ишга туширади, натижада вирус фойдаланувчи компьютеридан фойдалана олади.

Зарар келтирувчи дастурларни тарқатишнинг бошқа каналлари.

Вирусларни тарқатиш каналларидан бири дастурий таъминотнинг қароқчи нусхалари ҳисобланади. Дискетлар ва CD-дисклардаги ноқунуний нусхаларда кўпинча турли-туман вируслар билан заҳарланган файллар бўлади. Вирусларни тарқатиш манбаларига электрон анжуманлар ва FTP ва BBS файл-серверлар ҳам тааллуқли.

Ўқув юртларида ва Internet-марказларида ўрнатилган ва умумфойдаланиш режимида ишловчи компьютерлар ҳам осонгина вирусларни тарқатиш манбаига айланиши мумкин. Агар бундай компьютерлардан бири навбатдаги фойдаланувчи дискетидан заҳарланган бўлса, шу компьютерда ишловчи бошқа фойдаланувчилар дискетлари ҳам заҳарланади.

Компьютер технологиясининг ривожланиши билан компьютер вируслари ҳам, ўзининг янги яшаш маконига мослашган ҳолда, такомиллашади. Ҳар қандай онда янги, олдин маълум бўлмаган ёки маълум бўлган, аммо янги компьютер асбоб-ускунасига мўлжалланган компьютер вируслари, троян дастурлари ва қуртлар пайдо бўлиши мумкин. Янги вируслар маълум бўлмаган ёки олдин мавжуд бўлмаган тарқатиш каналларидан ҳамда компьютер тизимларга татбиқ этишнинг янги технологияларидан фойдаланиши мумкин. Вирусдан заҳарланиш хавфини йўқотиш учун корпоратив тармоқнинг тизим маъмури, нафақат вирусга қарши усуллардан фойдаланиши, балки компьютер вируслари дунёсини доимо кузатиб бориши шарт.

10.5. Вирусга қарши дастурлар

Компьютер вирусларини аниқлаш ва улардан ҳимояланиш учун махсус дастурларнинг бир неча хиллари ишлаб чиқилган бўлиб, бу дастурлар компьютер вирусларини аниқлаш ва йўқотишга имкон беради. Бундай дастурлар вирусга қарши дастурлар деб юритилади. Умуман, барча вирусга қарши дастурлар заҳарланган дастурларнинг ва юклама секторларнинг автоматик тарзда тикланишини таъминлайди.

Вирусларга қарши дастурлар фойдаланадиган вирусларни аниқлашнинг асосий усуллари қуйидагилар:

- эталон билан таққослаш усули;
- эвристик тахлил;
- вирусга қарши мониторинг;
- ўзгаришларни аниқловчи усул;
- компьютернинг киритиш/чиқариш базавий тизимига (BIOSга) вирусга қарши воситаларни ўрнатиш ва ҳ.

Эталон билан таққослаш усули энг оддий усул бўлиб, маълум вирусларни қидиришда ниқоблардан фойдаланади. Вируснинг ниқоби-мана шу муайян вирусга хос коднинг қандайдир ўзгармас кетма-кетлигидир. Вирусга қарши дастур маълум вирус ниқобларини қидиришда текширилувчи файлларни кетма-кет кўриб чиқади (сканерлайди). Вирусга қарши сканерлар фақат ниқоб учун белгиланган, олдиндан маълум вирусларни топа олади. Оддий сканерлар компьютерни янги вирусларнинг суқилиб киришидан ҳимояламайди. Янги дастурни ёки юклама секторини заҳарлашда кодини тўла ўзгартира олувчи шифрланувчи ва полиморф вируслар учун ниқоб ажратиш мумкин эмас. Шу сабабли сканер уларни аниқламайди.

Эвристик таҳлил. Компьютер вируси кўпайиши учун хотирада нусхаланиш, секторга ёзилиш каби қандайдир муайян харакатларни амалга ошириши лозим. Эвристик таҳлиллагичда бундай ҳаракатларнинг рўйхати мавжуд. Эвристик таҳлиллагич дастурларни ва диск ва дискет юклама секторларини, уларда вирусга хос кодларни аниқлашга уринган ҳолда, текширади. Тахлиллагич заҳарланган файлни топиб, монитор экранига ахборот чиқаради ва шахсий ёки тизимли журналга ёзади. Эвристик тахлил олдин маълум бўлмаган вирусларни аниқлайди.

Вирусга қарши мониторинг. Ушбу усулнинг моҳияти шундан иборатки, компьютер хотирасида бошқа дастурлар томонидан бажарилувчи шубҳали ҳаракатларни мониторингловчи вирусга қарши дастур доимо бўлади. Вирусга қарши мониторинг барча ишга туширилувчи дастурларни, яратилувчи, очилувчи ва сақланувчи хужжатларни, Internet орқали олинган ёки дискетдан ёки ҳар қандай компакт-дискдан нусҳаланган дастур ва хужжатларнинг файлларини текширишга имкон беради. Агар қандайдир дастур хавфли ҳаракатни қилишга уринмоқчи бўлса, вирусга қарши монитор фойдаланувчига хабар беради.

Ўзгаришларни аниқловчи усул. Дискни тафтиш қилувчи деб аталувчи ушбу усулни амалга оширишда вирусга қарши дастур дискнинг хужумга дучор бўлиши мумкин бўлган барча соҳаларини олдиндан хотирлайди, сўнгра уларни вақти-вақти билан текширади. Вирус компьютерларни заҳарлаганида қаттиқ диск таркибини ўзгартиради: масалан, дастур ёки

хужжат файлига ўзининг кодини қўшиб қўяди, Autoexec.bat файлига дастур-вирусни чақиришни қўшади, юклама секторни ўзгартиради, файл-йўлдош яратади. Диск соҳалари характеристикаларининг қийматлари солиштирилганида вирусга қарши дастур маълум ва ноъмалум вируслар томонидан қилинган ўзгаришларни аниқлаши мумкин.

Компьютерларнинг киритиш/чиқариш базавий тизимига (BIOSга) вирусга қарши воситаларни ўрнатиш. Компьютерларнинг тизимли платасига вируслардан ҳимоялашнинг оддий воситалари ўрнатилади. Бу воситалар қаттиқ дискларнинг бош юклама ёзувига ҳамда дисклар ва дискетларнинг юклама секторларига барча мурожаатларни назоратлашга имкон беради. Агар қандайдир дастур юклама секторлар таркибини ўзгартиришга уринса, ҳимоя ишга тушади ва фойдаланувчи огоҳлантирилади. Аммо бу ҳимоя жуда ҳам ишончли эмас.

Вирусга қарши дастурларнинг хиллари. Вирусга қарши дастурларнинг қуйидаги хиллари фарқланади:

- дастур-фаглар (вирусга қарши сканерлар);
- дастур-тафтишчилар (CRC-сканерлар);
- дастур-блокировка қилувчилар;
- дастур-иммунизаторлар.

Дастур-фаглар энг оммавий ва самарали вирусга қарши дастур ҳисобланади. Самарадорлиги ва оммавийлиги бўйича иккинчи ўринда дастур-тафтишчилар туради. Одатда, бу иккала дастур хиллари битта вирусга қарши дастурга бирлаштирилади, натижада унинг қуввати анчагина ошади. Турли хил блокировка қилувчилар ва иммунизаторлар ҳам ишлатилади.

Дастур-фаглар (сканерлар) вирусларни аниқлашда эталон билан таққослаш усулидан, эвристик тахлиллашдан ва бошқалардан фойдаланади. Дастур-фаглар оператив хотира ва файлларни сканерлаш йўли билан муайян вирусга характерли бўлган ниқобни қидиради. Дастур-фаглар нафақат вируслар билан заҳарланган файлларни топади, балки уларни даволайди ҳам, яъни файлдан дастур-вирус баданини олиб ташлаб, файлни дастлабки холатига қайтаради. Дастур-фаглар аввал оператив хотирани сканерлайди, вирусларни аниқлайди ва уларни йўқотади, сўнгра файлларни даволашга

киришади. Файллар ичида вирусларни катта сонини қидиришга ва йўқ қилишга аталган дастур-фаглар, яъни полифаглар ҳам мавжуд.

Дастур-фаглар иккита категорияга бўлинади: универсал ва ихтисослаштирилган сканерлар. Универсал сканерлар сканер ишлаши мўлжалланган операцион тизим хилига боғлиқ бўлмаган ҳолда, вирусларнинг барча хилларини қидиришга ва зарарсизлантиришга мўлжалланган. Ихтисослаштирилган сканерлар вирусларнинг чегараланган сонини ёки уларнинг бир синфини, масалан макровирусларни зарарсизлантиришга аталган. Фақат макровирусларга мўлжалланган ихтисослаштирилган сканерлар MS WORD ва Excel муҳитларида хужжат алмашиниш тизимини ҳимоялашда энг қулай ва ишончли ечим ҳисобланади.

Дастур-фаглар сканерлашни "бир зумда" бажарувчи мониторинглашнинг резидент воситаларига ва фақат сўров бўйича тизимни текширишни таъмнловчи резидент бўлмаган сканерларга ҳам бўлинади. Мониторинглашнинг резидент воситалари тизимни ишончлироқ ҳимоялашни таъминлайди, чунки улар вируслар пайдо бўлишига даров реакция кўрсатади, резидент бўлмаган сканер эса вирусни аниқлаш қобилиятига фақат навбатдаги ишга туширилишида эга бўлади.

Дастур-фагларнинг афзаллиги сифатида уларнинг универсаллигини кўрсатиш мумкин. Дастур-фагларнинг камчилиги сифатида вирусларни қидириш тазлигининг нисбатан катта эмаслигини ва вирусга қарши базаларнинг нисбатан катта ўлчамларини кўрсатиш мумкин. Ундан ташқари, янги вирусларнинг доим пайдо бўлиши сабабли дастур-фаглар тездан эскиради ва улар версияларининг мунтазам янгиланиши талаб этилади.

Дастур-тафтишчилар (CRC-сканерлар) вирусларни қидиришда ўзгаришларни аниқловчи усулдан фойдаланади. CRC-сканерлар дискдаги файллар/тизимли сектордагилар учун CRC-йиғиндини (циклик назорат кодини) ҳисоблашга асосланган. Бу CRC-йиғиндилар вирусга қарши маълумотлар баъзасида файллар узунлиги, саналар ва охирги модификацияси ва бошқа параметрлар хусусидаги қўшимча ахборотлар билан бир қаторда сақланади. CRC-сканерлар ишга туширилишида маълумотлар базасидаги маълумот билан реал ҳисобланган қийматларни таққослайди. Агар маълу-

мотлар базасидаги ёзилган файл хусусидаги ахборот реал қийматларга мос келмаса, CRC-сканерлар файл ўзгартирилганлиги ёки вирус билан заҳарланганлиги хусусида хабар беради. Одатда холатларни таққослаш операцион тизим юкланишдан сўнг дарҳол ўтказилади.

CRC-сканерларнинг камчилиги сифатида уларнинг янги файллардаги вирусларни аниқлай олмаслигини кўрсатиш мумкин, чунки уларнинг маълумотлар базасида бу файллар хусусидаги ахборот мавжуд эмас.

Дастур-блокировка қилувчилар вирусга қарши мониторинглаш усулини амалга оширади. Вирусга қарши блокировка қилувчилар резидент дастурлар бўлиб, вирус хавфи вазиятларини тўхтатиб қолиб, у хусусида фойдаланувчига хабар беради. Вирус хавфи вазиятларига вирусларнинг кўпайиши онларидаги характерли чақириқлар киради. Блокировка қилувчиларнинг афзалликлари сифатида вируслар кўпайишининг илк босқичида уларни тўхтатиб қолишини кўрсатиш мумкин. Бу айниқса, кўпдан бери маълум вируснинг мунтазам пайдо бўлишида муҳим ҳисобланади. Аммо, улар файл ва дискларни даволамайди. Блокировка қилувчиларнинг камчилиги сифатида улар ҳимоясининг айланиб ўтиш йўлларининг мавжудлигини ва уларнинг "хираликлигини" (масалан, улар бажарилувчи файлларнинг ҳарқандай нусхаланишига уриниш хусусида мунтазам огоҳлантиради) кўрсатиш мумкин. Таъкидлаш лозимки, компьютер аппарат компоненти сифатида яратилган вирусга қарши блокировка қилувчилар мавжуд.

Дастур-иммунизаторлар – файллар заҳарланишини олдини олувчи дастурлар икки хилга бўлинади: заҳарланиш хусусида хабар берувчи ва вируснинг қандайдир хили бўйича заҳарланишни блокировка қилувчи. Биринчи хил иммунизаторлар, одатда, файл охирига ёзилади ва файл ишга туширилганда ҳар марта унинг ўзгаришини текширади. Бундай иммунизаторлар битта жиддий камчиликка эга. Улар стелс-вирус билан захарланишни аниқлай олмайдилар. Шу сабабли бу хил иммунизаторлар ҳозирда ишлатилмайди.

Иккинчи хил иммунизаторлар тизимни вируснинг маълум тури билан заҳарланишдан ҳимоялайди. Бу иммунизатор дастур ёки дискни шундай мо-

дификациялайдики, бу модификациялаш уларнинг ишига таъсир этмайди, вирус эса уларни заҳарланган деб қабул қилади ва суқилиб кирмайди. Иммунизациялашнинг бу хили универсал бўлаолмайди, чунки файлларни барча маълум вируслардан иммунизациялаш мумкин эмас. Аммо бундай иммунизаторлар чала чора сифатида компьютерни янги ноъмалум вирусдан, у вирусга қарши сканерлар томонидан аниқланишига қадар, ишончли ҳимоялаши мумкин.

Вирусга қарши дастурнинг сифат мезонлари. Вирусга қарши дастурни бир неча мезонлар бўйича баҳолаш мумкин. Қуйида бу мезонлар муҳимлиги даражаси пасайиши тартибда келтирилган:

- ишончлилик ва ишлаш қулайлиги фойдаланувчилардан махсус ҳаракатларни талаб этувчи техник муаммоларнинг йўқлиги; вирусга қарши дастурнинг ишончлилиги энг муҳим мезон ҳисобланади, чунки ҳатто энг яхши вирусга қарши дастур сканерлаш жараёнини охиригача олиб бора олмаса, у бефойда ҳисобланади;

- вирусларни барча тарқалган хилларини аниқлаш фазилати, ички файл-хужжатлар/жадвалларни (MS Office), жойлаштирилган ва архивланган файлларни сканерлаш, вирусга қарши дастурнинг асосий вазифаси-100% вирусларни аниқлаш ва уларни даволаш;

- барча оммавий платформалар (DOS, Windows 95/NT, Novell NetWare, OS/2, Alpha, Linux ва ҳ.) учун вирусга қарши дастур версияларининг мавжудлиги; сўров бўйича сканерлаш ва "бир зумда" сканерлаш режимларининг борлиги, тармоқни маъмурлаш имкониятли сервер версияларининг мавжудлиги. Вирусга қарши дастурнинг кўп платформалилиги муҳим мезон ҳисобланади, чунки муайян операцион тизимга мўлжалланган дастургина бу тизим функцияларидан тўла фойдаланиш мумкин. Файлларни "бир зумда" текшириш имконияти ҳам вирусга қарши дастурларнинг етарлича муҳим мезони ҳисобланади. Компьютерга келувчи файлларни ва қўйилувчи дискетларни бир лаҳзада ва мажбурий текшириш вирусдан заҳарланмасликка 100%-ли кафолат беради. Агар вирусга қарши дастурнинг сервер вариантида тармоқни маъмурлаш имконияти бўлса, унинг қиймати янада ошади.

- ишлаш тезлиги. Вирусга қарши дастурнинг ишлаш тезлиги ҳам унинг муҳим мезони ҳисобланади. Турли вирусга қарши дастурларда вирусни қидиришнинг ҳар хил алгоритмларидан фойдаланилади. Бир алгоритм тезкор ва сифатли бўлса, иккинчиси суст ва сифати паст бўлиши мумкин.

Ҳимоянинг профилактика чоралари. Ҳар бир компьютерда вируслар билан заҳарланган файллар ва дискларни ўз вақтида аниқлаш, аниқланган вирусларни тамомила йўқотиш вирус эпидемиясининг бошқа компьютерларга тарқалишининг олдини олади. Ҳар қандай вирусни аниқлашни ва йўқ қилишни кафолатловчи мутлоқ ишончли дастурлар мавжуд эмас. Компьютер вируслари билан курашишнинг муҳим усули ўз вақтидаги профилактика ҳисобланади.

Вирусдан заҳарланиш эҳтимоллигини жиддий камайтириш ва дисклардаги ахборотни ишончли сақланишини таъминлаш учун қуйидаги профилактика чораларини бажариш лозим:

- фақат қонуний, расмий йўл билан олинган дастурий таъминотдан фойдаланиш;

- компьютерни замонавий вирусга қарши дастурлар билан таъминлаш ва улар версияларини доимо янгилаш;

- бошқа компьютерларда дискетда ёзилган ахборотни ўқишдан один бу дискетда вирус борлигини ўзининг компьютеридаги вирусга қарши дастур ёрдамида доимо текшириш;

- ахборотни иккилаш. Аввало дастурий таъминотнинг дистрибутив элтувчиларини сақлашга ва ишчи ахборотни сақланишига эътибор бериш;

- компьютер тармоқларидан олинувчи барча бажарилувчи файлларни назоратлашда вирусга қарши дастурдан фойдаланиш;

- компьютерни юклама вируслардан заҳарланишига йўл қўймаслик учун, операцион тизим ишга туширилганида ёки қайта юкланишида дисковод чўнтагида дискетани қолдирмаслик.

Вирусга қарши дастурларнинг ҳар бири ўзининг афзалликларига ва камчиликларига эга. Фақат вирусга қарши дастурларнинг бир неча хилини комплекс ишлатилиши мақбул натижага олиб келиши мумкин.

Қуйида вирусдан заҳарланиш профилактикасига, вирусларни аниқлаш ва йўқотишга мўлжалланган баъзи дастурий комплекслар тавсифланган.

AVP (Антивирус Касперского Personal) – Россиянинг вирусга қарши пакети. Пакет таркибига қуйидагилар киради:

- Office Guard – блокировка қилувчи, макровирусдан 100% ҳимояланишни таъминлайди;

- Inspector – тафтишчи, компьютердаги барча ўзгаришларни кузатади, вирус фаоллиги аниқланганида дискнинг асл нусхасини тиклашга ва зарар келтирувчи кодларни чиқариб ташлашга имкон беради;

- Monitor – вирусларни ушлаб қолувчи, компьютер хотирасида доимо ҳозир бўлиб, файллар ишга туширилганида, яратилишида ёки нусхаланишида уларни вирусга қарши текширади;

- Scanner – вирусга қарши модул, локал ва тармоқ дисклар таркибини кенг кўламли текшириш имконини беради. Сканерни қўл ёрдамида ёки берилган вақтда автоматик тарзда ишга тушириш мумкин.

Пакет ёрдамида электрон постани вирусга қарши фильтрлаш ва почта корреспонденциясини комплекс текшириш амалга оширилади. Вирусга қарши базани янгилаш Internet орқали бажарилади.

Dr.Web – Россиянинг вирусга қарши оммавий дастури, Windows 9x/NT/2000/XP учун мўлжалланган бўлиб, файлли, юклама, ва файл-юклама вирусларни қидиради ва зарарсизлантиради. Дастур таркибида резидент қоровул SpIDer Guard, Internet орқали вирус базаларини янгилашнинг автоматик тизими ва автоматик текшириш жадвалини режалаштирувчи мавжуд. Почта файлларини текшириш амалга оширилган.

Dr.Web да ишлатилувчи алгоритмлар ҳақида маълум бўлган барча вирус хилларини аниқлашга имкон беради. Dr.Web дастурининг муҳим хусусияти – оддий сигнатурли қидириш натижа бермайдиган мураккаб шифрланган ва полиморф вирусларни аниқлаш имкониятидир.

Symantec Antivirus – Symantec компаниясининг корпоратив фойдаланувчиларга таклиф этган вирусга қарши маҳсулоти тўплами.

Symantec маҳсулотидан ишчи жойларининг умумий сони 100 ва ундан ортиқ бўлганида ва бўлмаганда битта Windows NT/2000/NetWare серве-

ри мавжудлигида фойдаланиш мақсадга мувофиқ ҳисобланади. Ушбу пакетнинг башқалардан ажралиб турадиган хусусияти қуйидагилар:

- бошқаришнинг иерархик модели;

- янги вирус пайдо бўлишига реакция қилиш механизмининг мавжудлиги.

AntiVir Personal Edition – вирусга қарши дастур AVP, Dr.Web ва ҳ.лар имкониятларидек имкониятларга эга. Дастур комплектига қуйидагилар киради:

- дискларни сканерловчи;

- резидент қоровул;

- бошқариш дастури;

- режалаштирувчи.

Дастур Internet дан юкланувчи файлларни сканерлайди. Internet орқали янгиланишларни автоматик тарзда текшириш ва юклаш функцияси ҳам мавжуд. Дастур хотирани, юкланиш секторини текширишда ва унда вируслар бўйича кенг кўламдаги маълумотнома мавжуд.

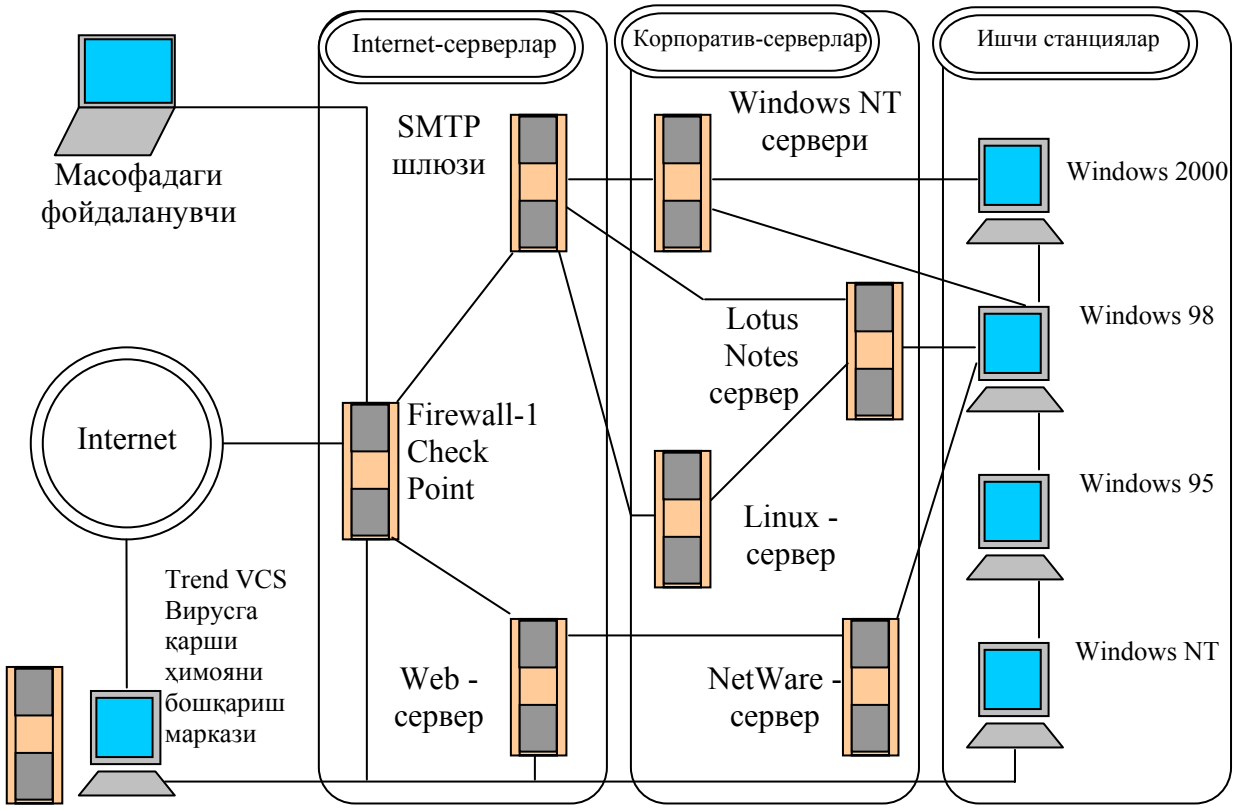
10.6. Вирусга қарши ҳимоя тизимини қуриш

Ҳозирда ўртача компаниянинг корпоратив компьютер тармоғи таркибида ўнлаб ва юзлаб ишчи станциялари, ўнлаб серверлар, телекоммуникациянинг турли фаол ва пассив асбоб ускуналари мавжуд бўлган етарлича мураккаб тузилмага эга (10.6-расм).

Корпоратив тармоқдан фойдаланувчилар тармоққа вирусларнинг суқилиб кириш файллари билан доимо тўқнашадилар. Internet/intranet корпоратив тизимларига вирус хужумлари мунтазам бўлиб туради, фойдаланувчи ишчи станциясининг заҳарланган ахборот элтувчиси томонидан заҳарланиши эса одат тусини олган.

Корпоратив тармоқ вируслар ва бошқа зарар келтирувчи дастурлар хужумларига дучор бўлганида тармоқнинг вирусга қарши ҳимояси кўпинча вирусга қарши локал дастурий таъминот ёрдамида, сканерлаш ва қатор ишчи станцияларни даволаш билан тугайди ва ҳимоя таъминланади деб

ҳисобланади. Аслида муаммонинг бундай локализациялаш минимал чора ҳисобланади ва корпоратив тармоқнинг кейинги барқарор ишлашини кафолатламайди. Бошқача айтганда, вирусга қарши локал ечимларнинг ишлатилиши корхонани вирусдан самарали ҳимоялаш учун зарурий, аммо етарли восита ҳисобланмайди.



10.6–расм. Корпоратив тармоқ намунавий архитектураси

Вирусга қарши ҳимоянинг самарали корпоратив тизими-"мижоз-сервер" технологияси бўйича амалга оширилган, тармоқдаги ҳар қандай шубҳали ҳаракатни сезгирлик билан фаҳмлаб олувчи, тескари боғланишли мосланувчан тизимдир. Бундай тизим корпоратив тармоқнинг ички тузилмаси доирасида вирусларни ва бошқа ғаним дастурларнинг тарқалишига йўл қўймайди. Вирусга қарши ҳимоянинг самарали корпоратив тизими турли вирус хужумларини-маълумларини, ҳам номаълумларини, улар намоён бўлишининг дастлабки босқичида, аниқлайди ва бетарфлаштиради.

Албатта, турли вазиятлар бўлиши мумкин, масалан масофадан фойдаланувчининг заҳарланган компьютерини корпоратив серверга улаганда ёки макровируслар бўлган WORD ёки Excel файлли дискетлардан иш жойларида фойдаланишда тармоқ заҳарланиши мумкин. Аммо, сифатли қурилган

вирусга қарши ҳимоянинг корпоратив тизими учун бу жиддий эмас, чунки, биринчидан, заҳарланишнинг кўрсатилган ҳолатлар камдан-кам учрайди, иккинчидан, вируслар вақтида аниқланади ва бетарафлаштирилади. Натижада уларнинг кўпайишига ва корпоратив тармоқ доирасида тарқалишига йўл қўйилмайди.

Уланадиган ишчи станциялари сони ошган сари корпоратив тармоқнинг хизмат кўрсатиш нархи оша боради. Корпоратив тармоқни вируслардан ҳимоялаш харажатлари корхона умумий харажатлари рўйхатида охирги бандини эгалламайди.

Ушбу харажатларни корпоратив тармоқни вирусга қарши ҳимоялашни вақтнинг реал масштабида марказлаштирилган бошқариш орқали оптималлаштириш ва камайтириш мумкин. Бундай ечим корхона тармоғи маъмурларига вирусни барча суқилиб кириш нуқталарини бошқаришнинг ягона консоли орқали кузатишга ва корпоратив тармоқдаги барча вирусга қарши воситаларни самарали бошқаришга имкон беради. Вирусга қарши ҳимояни марказлаштирилган бошқариш мақсади жуда оддий – вирусларнинг барча суқилиб кириш нуқталарини блокировка қилиш. Қуйидаги суқилиб киришларни ва захарланишларни кўрсатиш мумкин:

- ташувчи манбалардан (флоппи-дисклар, компакт-дисклар, Zip, Jazz, Floptical ва ҳ.) охирги заҳарланган файллардан фойдаланишда ишчи станцияларга вирусларнинг суқилиб кириши;

- Internetдан Web ёки FTP орқали олинган локал ишчи станциясида сақланган заҳарланган текин дастурий таъминот ёрдамида заҳарланиш;

- масофадаги ёки мобил фойдаланувчиларнинг заҳарланган ишчи станциялари корпоратив тармоққа уланганида вирусларнинг суқилиб кириши;

- корпоратив тармоққа уланган масофадаги сервердаги вируслар билан заҳарланиш.

- иловаларида макровируслар билан заҳарланган Excel ва Word файллар бўлган электрон почтанинг тарқалиши.

Вируслардан ва бошқа зарар келтирувчи дастурлардан ҳимояловчи корпоратив тизимни қуриш қуйидаги босқичларни ўз ичига олади.

Биринчи босқичда ҳимояланувчи тармоқнинг ўзига хос хусусиятлари аниқланади ва бир неча вирусга қарши ҳимоя вариантлари танланади ва асосланади. Бу босқичда қуйидагилар бажарилади:

- компьютер тизими ва вирусга қарши ҳимоя воситаларининг аудити;
- ахборот тизимини текшириш ва *картирлаш*;
- вирусларнинг суқилиб кириши билан боғлиқ таҳдидларнинг амалга ошириш сценарийсини тахлиллаш.

Натижада вирусга қарши ҳимоянинг умумий ҳолати баҳоланади.

Иккинчи босқичда вирусга қарши хавфсизлик сиёсати ишлаб чиқилади. Бу босқичда қуйидагилар бажарилади:

- ахборот ресурсларини туркумлашнинг тури;
- вирусга қарши хавфсизликни таъминловчи кучларни яратиш- вакалатларни тақсимлаш;
- вирусга қарши хавфсизликни ташкилий-хуқуқий мададлаш;
- вирусга қарши хавфсизлик инструментларига талабларни аниқлаш;
- вирусга қарши хавфсизликни таъминлаш харажатларини ҳисоблаш.

Натижада корхонанинг вирусга қарши хавфсизлик сиёсати ишлаб чиқилади.

Учинчи босқичда дастурий воситалари, ахборот ресурсларини инвентаризациялаш ва мониторингини автоматлаштириш воситалари танланади. Вирусга қарши хавфсизликни таъминлаш бўйича ташкилий тадбирлар рўйхати ишлаб чиқилади.

Натижада корхонанинг вирусга қарши хавфсизлигини таъминловчи режа ишлаб чиқилади.

Тўртинчи босқичда вирусга қарши танланган ва тасдиқланган хавфсизлик режаси амалга оширилади. Бу босқичда вирусга қарши воситалар етказиб берилади, жорий этилади ва мададланади.

Натижада корпоратив вирусга қарши ҳимоялашнинг самарали тизими яратилишига имкон туғилади.

XI боб. МАЪЛУМОТЛАРНИ УЗАТИШ ТАРМОҒИДА АХБОРОТНИ ҲИМОЯЛАШ

11.1. Маълумотларни узатиш тармоқларида ахборот ҳимоясини таъминлаш

Маълумотларни узатиш тармоқларида ахборот ҳимоясини таъминлаш масаласи маълумотлар узатиш тармоғининг муайян архитектурасини амалга оширувчи ва унинг барқарор ишлашини таъминловчи аппарат-дастурий воситалари билан боғлиқ ҳолда ечилиши лозим.

Маълумотларни узатиш тармоқларида ахборот хавфсизлигини таъминлашга қуйидаги талаблар қуйилади:

- маълумотларни узатиш тармоқларида ахборот хавфсизлигига бўладиган маълум таҳдидлардан ҳимоялаш хизмати ва механизмларини белгиловчи *функционал талаблар*;

- ахборот хавфсизлигига бўладиган маълум таҳдидлардан ҳимоялаш механизмини маълумотларни узатиш тармоғи архитектурасига қай тарзда жорий этилиши лозимлигини белгиловчи *архитектуравий талаблар*;

- бошқаришнинг қандай функциялари ишлаб чиқилиши ва улар қай тарзда маълумотларни узатиш тармоғига жорий этилишини белгиловчи *бошқариш (маъмурлаш) талаблари*.

Функционал талаблар. Маълумотларни узатиш тармоғи компонентларига ва архитектурасига реал таъсир этувчи умумий функционал талаблар қуйидагилар:

- *фойдаланувчини аутентификациялаш.* Маълумотларни узатиш тармоғида ахборот хавфсизлигини таъминловчи тизим ахборотни (маълумотларни) узатиш жараёнида иштирок этувчи компонентининг (объект, субъект ва фойдаланувчининг) ҳақиқийлигини аниқлаш имкониятини таъминлаши лозим;

- *назоратланувчи фойдаланиш.* Маълумотларни узатиш тармоғида ахборот хавфсизлигини таъминловчи тизим тармоқ субъектлари ва фойдала-

нувчиларининг рухсат этилмаган ахборот ресурсларидан фойдалана олмасликларини кафолатлаши лозим;

- *конфиденциалликни таъминлаш.* Конфиденциалликни таъминлаш хизмати асосан маълумотларни узатиш тармоғини ахборот муҳитини очиш, ахборотдан рухсатсиз фойдаланиш ва ўғирлаш имкониятларидан ҳимоялаш учун зарур ҳисобланади;

- *маълумотлар яхлитлигини таъминлаш.* Маълумотларни узатиш тармоғида ахборот хавфсизлигини таъминловчи тизим таркибида фойдаланувчи ва бошқариш ахбороти бўлган маълумотларнинг сақланиш ва узатилиш яхлитлигини кафолатлаши лозим. Маълумотларнинг бузилиши, сохталаштирилиши, кечиктирилиши, рухсатсиз қайталаниши ахборот узатилишининг блокировка қилинишига олиб келиши мумкин;

- *қатъий ҳисоб-китоб*. Маълумотларни узатиш тармоғи ресурсларидан фойдаланувчи ҳар қандай субъект бажарган ҳар қандай амаллари учун жавоб бериши лозим. Маълумотларни узатиш тармоғи устида қилинган барча ҳаракатлар ва тармоқда содир бўлган барча ходисалар хусусидаги ахборотнинг сақланиш имконияти таъминланиши лозим;

- *хавфни билдирувчи сигнални генерациялаш*. Маълумотларни узатиш тармоғи тармоқ ахборот хавфсизлиги объектлари томонидан хавфсизликнинг бузилиши хусусидаги сигнални генерациялаш имконини таъминлаши лозим;

- *аудит.* Аудит тизимни бошқаришнинг самарадорлигини баҳолаш ҳамда ахборот хавфсизлигининг бузилишини аниқлаш мақсадида тизимли ёзувларни ва амалларни мустақил тахлиллаш ва тадқиқлаш сифатида кўрилиши лозим;

- *тиклаш.* Маълумотларни узатиш тармоғида ахборот хавфсизлигини таъминлаш тизими хавфсизликнинг бузилишини тиклаш қобилиятига эга бўлиши лозим. Ҳар доим, қачон ахборот хавфсизлигини бузишга уриниш содир бўлганида, тизим ушбу уриниш хусусидаги ахборотни шундай ишлаши лозимки, ушбу уриниш маълумотларни узатиш тармоғининг ўтказиш қобилиятини ва фойдаланувчанлигини жиддий пасайишига олиб келмасин;

- *мосланувчанлик.* Маълумотларни узатиш тармоғида ахборот хавфсизлигини таъминлаш тизимига қуйиладиган муҳим концептуал талаб-мосланувчанлик талаби, яъни алоқа тармоғининг тузилмаси, технологияси ва ишлаш шароити ўзгарганида мослашув қобилияти талабидир.

Архитектуравий талаблар. Маълумотларни узатиш тармоғида ахборот хавфсизлигини таъминлаш тизими ахборот хавфсизлигининг турли сиёсатини мададлаши, яъни мосланувчан бўлиши лозим. Тизимга қйидаги асосий хизматлар киритилиши мумкин:

- шифрлаш калитларини ва паролларни шакллантириш, сақлаш ва тақсимлаш хизмати;
- шифрлаш хизмати;
- фойдаланувчиларни ва хабарларни аутентификациялаш хизмати;
- фойдаланишни бошқариш хизмати;
- хабарлар яхлитлигини таъминлаш хизмати;
- фойдаланувчанликни таъминлаш хизмати;
- етказилганликни тасдиқлаш хизмати;
- рад қилмаслик хизмати;
- қўшимча трафикни шакллантириш хизмати;
- маъмурлаш хизмати.

Бу хизматларнинг ҳар бири ахборот хавфсизлигини таъминлаш бўйича масалаларни мустақил тарзда у ёки бу ҳимоя механизмларидан фойдаланиб ечиши мумкин. Бунда ҳимоянинг битта механизми ахборот хавфсизлигининг турли хизматларида қўлланилиши мумкин.

Бошқариш (маъмурлаш) талаблари. Маълумотларни узатиш тармоғида ахборот хавфсизлигини маъмурлаш хизмати ҳимоянинг техник воситаларини тўлдирувчи ҳимоя чораларининг маълум комплексини ўз ичига олади. Бу ҳимоя чоралари бузғунчининг тармоқ ахборот хавфсизлигига таҳдидни кучайтиришга қаратилган у ёки бу таъсирни ўтказишини қийинлаштириш мақсадида мавжуд ҳимоя тизимига оператив тарзда ўзгартиришлар киритишга имкон яратади.

Маъмурлаш хизматининг асосий вазифалари қуйидагилар:

- ҳимоя хизмати ва механизмига зарур ахборотни тарқатиш;

- ҳимоя хизмати ва механизмининг ишлаши хусусидаги ахборотни йиғиш ва тахлиллаш;

- ҳимояланувчи объектларни аниқлаш;

- хизмат функцияларини самарали амалга ошириш мақсадида ҳимоя механизмларини комбинациялаш;

- маълумотларни узатиш тармоғининг ишончли ва барқарор ишлашини таъминлаш хизматларига жавобгар бошқа маъмурлар билан ўзаро алоқа;

-маълумотларни узатувчи тармоқнинг бузилган ишлаш жараёнини тиклаш.

Хавфсизлик маъмури маъмурлаш хизматининг муҳим элементи ҳисобланади. Ахборот хавфсизлигининг ҳар қандай воситаларидан фойдаланилмасин, маълумотларни узатиш тармоғида ахборот хавфсизлигини таъминлаш сифати маъмурнинг қобилиятига, унинг тиришишига, техник жихозланганлигига боғлиқ.

Таъкидлаш лозимки, бирорта ҳам реал ҳимояланган маълумотларни узатиш тармоғи мутлоқ ҳимояланган бўлмайди. Шунга қарамасдан ҳимоянинг адекват чоралари бузғунчи таъсири самарасини (зарар келтириш ҳаражатининг кутилаётган зарар ўлчамига нисбатини) анчагина пасайтиради.

11.2. Алоқа каналларида маълумотларни ҳимоялаш усуллари

Маълумотларни узатишни ҳимоялаш масаласини ечиш усулларининг учта асосий гуруҳи мавжуд: каналга мўлжалланган ҳимоялаш усуллари, чеккалараро ҳимоялаш усуллари ва уланишга мўлжалланган ҳимоялаш усуллари. Биринчиси ҳар бир канал учун мустақил равишда маълумотлар оқимини ҳимоялашни таъминласа, иккинчиси ҳар бир хабарни, уни манбадан адресатгача узатишда умумий ҳимоялашни таъминлайди. Учинчи усул иккинчи усулнинг бир тури ҳисобланади.

Каналга мўлжалланган усуллар манба ва адресатга боғлиқ бўлмаган ҳолда, алоҳида узеллар орасидаги алоҳида алоқа канали бўйича узатилаётган хабарлар оқимини ҳимоялашни таъминлайди. Бу хил ҳимояни таъмин-

лашда бузғунчининг узелга (пакетни коммутацияловчи марказга) қараганда каналга таъсир этиш қулайлиги фараз қилинади. Ундан ташқари, маълумотларни узатиш тармоғидаги узелларни фойдаланувчи терминалларини ҳимоялагандек ҳимоялаш мумкин эмас ёки иқтисод нуқтаи назаридан фойдасиз. Ушбу гуруҳ усулларининг камчилиги-қисм тармоқ узелларидан бирининг очилиши тармоқ орқали ўтаётган хабарлар оқимининг талайгина қисмини очилишига олиб келиши мумкин.

Терминаллар ва тармоқлар ўртасидаги алоқа каналларини каналга мўлжалланган ҳимоялаш ҳаражатлари бевосита дахлдор тарафлар томонидан қоплансада, маълумотларни узатиш қисм тармоғи ичидаги каналга мўлжалланган ҳимоялаш усулларининг умумий нархи қисм тармоқдан фойдаланувчиларнинг барчаси ўртасида ҳисоблаб чиқилиши мумкин.

Чеккалараро ҳимоялаш усуллари хабарларни манба узеллари ва қабул қилувчи орасида узатиш жараёнида шундай ҳимоялайдики, манба ва адресат орасидаги алоқа каналларидан бирининг очилиши хабарлар оқимининг очилишига олиб келмайди. Ушбу усулларнинг асосий афзаллиги – улардан фойдаланиш масаласи алоҳида фойдаланувчилар орасида, бошқа фойдаланувчиларни жалб этмасдан, ечилиши мумкин.

Уланишга мўлжалланган усуллар. Аксарият қўлланиш соҳаларида маълумотларни узатиш тармоғини манбадан адресатгача уланишни ёки виртуал канални ўрнатиш учун фойдаланувчига тақдим этилувчи муҳит сифатида тасаввур этиш мумкин. Бундай тасаввур этишда ҳимоя уланишга мўллжалланиши фараз қилинади, яъни, ҳар бир уланиш ёки виртуал канал алоҳида ҳимояланади. Шундай қилиб, уланишга мўлжалланган усуллар чеккалар аро ҳимоялаш усулларининг бир тури ҳисобланади. Уланишга мўлжалланган усуллар турли шароитларда умумий ҳимоянинг юқори даражасини таъминлайди ва ҳимояга қуйиладиган талаблар хусусидаги фойдаланувчининг идрокига мос келади. Чунки, уланишга мўлжалланган ахборот конфиденциаллигини ҳимоялаш усуллари асбоб-ускунани ҳимоялашни, масалан, фақат хабарлар манбаида ва қабул қилувчида ахборотдан рухсатсиз фойдаланишдан ҳимоялашни кўзда тутади. Айни вақтда ҳимоялашнинг каналга мўлжалланган усуллари рухсатсиз фойдаланишдан ҳимоялашнинг

маълумотларни узатиш тармоғидаги ҳар бир узели томонидан таъминланишини талаб этиши мумкин. аммо, баъзида иккала усулни қўллаганда ҳимоялашнинг тежамли даражасига эришилади.

Маълумотларни узатишни ҳимоялашнинг у ёки бу усулидан фойдаланишдаги асосий вазифалар қуйидагилар:

- хабарлар мазмунининг фош қилинишини олдини олиш;
- хабарлар оқимининг тахлилланишини олдини олиш;
- хабарлар оқими ҳақиқийлигини бузилганлигини аниқлаш;
- ёлғон уланишни аниқлаш.

Ахборот тизимлари ёки маълумотларни узатиш тармоқларида ахборот хавфсизлигини таъминлаш мақсадида маълумотларни узатишни ҳимоялаш усулларидан нафақат бузғунчи таъсири оқибатларини аниқлашни, балки, агар оқибатлар вақтинча характерга эга бўлганида, узилган (бузилган) узатиш жараёнини автоматик тарзда тиклашни талаб этиш керак.

Ҳозирда юқорида келтирилган вазифаларнинг бажарилишини таъминловчи ҳимоялашнинг стандартлаштирилган механизмлари мавжуд эмас. Ҳар бир муайян ҳолда маълумотларни узатиш хавфсизлиги масалалари ахборотларни криптографик ўзгартириш усуллари, ахборотларни ҳалалларга бардош кодлаш усуллари, хабарларнинг ҳақиқийлигини таъминловчи усуллар, тизимлар ишлашининг ишончлилигини, яшовчанлигини ва барқарорлигини таъминловчи усулларга асосланган ҳимоялашнинг турли механизмларини биргаликда ишлатиш орқали ҳал этилади.

Хабарлар мазмунининг фош қилинишини олдини олишда ҳимоялашнинг каналга мўлжалланган ҳамда уланишга мўлжалланган усулларидан фойдаланиш мумкин.

Юқорида айтиб ўтилганидек, каналли шифрлаш алоқа тармоғининг ҳар бир каналида мустақил тарзда бажарилиши мумкин. Каналли шифрлашда, одатда, оқимли шифрлаш ишлатилади ва узеллар орасида шифрланган матн битларининг узлуксиз оқими мададланади. Тармоқларда коммутациялаш (маршрутлаш) вазифалари фақат узелларда бажарилиши сабабли, алоқа каналида пакетнинг сарлавҳалари билан бирга ахборот қисмини ҳам шифрлаш мумкин.

Аммо маълумотлар фақат каналда (каналлар орқали уланган узелларда эмас) шифрланиши сабабли барча оралиқ узеллар ҳимояланиши лозим. Бунинг устига узелларни нафақат физик ҳимояланиши, балки бу узелларнинг аппарат-дастурий воситалари томнидан узеллар орқали ўтувчи ҳар бир уланишдаги ахборотни яккалаши кафолатланиши зарур.

Чеккалар аро шифрлашда маршрутизаторда ишланувчи ҳар бир хабар (сарлавҳанинг баъзи маълумотлари бундан истисно) йўл бошида шифрланади ва белгиланган жойга етмагунча расшифровка қилинмайди. Ҳар бир уланиш учун ўзининг калити ишлатилиши мумкин.

Хабарлар оқимини тахлилланишидан ҳимоялаш, одатда, турли синфларга мансуб хабарлар узунлиги ва частотасининг қийматларини, манба адресларини ва хабарлар оқими адресларини беркитишга йўналтирилган. Агар каналли шифрлаш ишлатилса, узеллар орасида маълумотлар узатилганида шифрланган матн битларининг узлуксиз оқими ўрнатилиши мумкин. Бу эса частота қийматларини ва уланишнинг давомлигини беркитишга имкон беради. Бундай ёндашишда тармоқнинг самарали ўтказиш қобилияти пасаймайди, чунки ҳеч қандай қўшимча ахборот талаб этилмайди. Аммо, узел очилса бу узел орқали утувчи хабарларнинг бутун оқими тахлиллаш мавзуига айланади.

Ҳимоялашнинг чеккалараро усулларидан фойдаланилганда узатилувчи хабарларнинг ҳақиқий частотаси ва узунлигини беркитиш учун турли узунликдаги "бўш" хабарлар генерацияланиши, ҳақиқий хабар эса бўш символлар билан тўлдирилиши мумкин. Қабул қилувчи бегона кенгайишларни ва "бўш" хабарларни аниқлашда хабардаги шифрланган ҳошиядан фойдаланиши мумкин.

Аксарият иловаларда оқимни тахлиллаш орқали ахборотни чиқариб олиш иккинчи даражали хавф сифатида талқин қилиниши ва махсус қарши чоралар кўрилмаслиги мумкин.

Хабарлар сатҳида ҳақиқийликни тасдиқлаш хабарларни кечиктириш, уларни йўқ қилиш, алмаштириб қўйиш ёки қайталаш каби таъсирлардан ҳимоялашни таъминламайди. Шунга қарамасдан, бундай таҳдидлардан ҳимоялашнинг турли усуллари мавжуд:

- хабарларни номерлаш. Ҳар бир хабарни номерлаб, номерни хабар таркибига киритиб, демак, шифрлаб узатиш орқали хабарнинг ҳақиқийлигига ишонч ҳосил қилиш мумкин. Тармоқнинг ҳар бир объекти у билан алоқада бўлувчи объектларнинг ҳар бири учун алоҳида санагичларга (счетчикларга) эга бўлиши лозимлиги бу муолажанинг камчилиги ҳисобланади.

- вақтни белгилаш. Қабул қилувчи ҳар бир узатилган хабарнинг куни ва вақтини билган ҳолда унинг адекватлигини текшириши мумкин. Бундай белгилашнинг интервали ва аниқлиги шундай танланиши лозимки, бир томондан ҳатоли хабарлар, иккинчи томондан узатиш каналига хос бўлган табиий кечикиш аниқланиши мумкин бўлсин.

- тасодифий сонлардан фойдаланиш. Вақтнинг реал масштабида икки томонлама алоқа ишлатилганида қабул қилувчи жўнатувчига хабар жўнатилмасдан олдин тасодифий сон юборади. Жўнатувчи бу сонни шифрланган хабарга шундай ўрнатадики, қабул қилувчи уни текшириши мумкин бўлсин. Шу тарзда ёлғон хабарлар чиқариб ташланиши мумкин.

- ҳар бир уланиш учун алоҳида калитдан фойдаланиш. Натижада олинган хабарда уланишнинг ошкор бўлмаган идентификацияланиши амалга оширилади.

Хабарлар оқими узилишини аниқлаш масаласини "сўров-жавоб" протоколидан фойдаланиб ҳал этиш мумкин. Бундай протоколнинг таркибида уланишнинг вақтинчалик яхлитлигини ва мақомини ўрнатувчи хабарлар жуфтини алмашиш муолажаси бўлади. Уланишнинг ҳар бир чеккасида "хабар-сўров" узатишни вақти-вақти билан ишга туширувчи таймер ишлатилади ва "хабар-сўров" узатишга уланишнинг бошқа чеккасидан жавоб олинади. Ҳар бир "хабар-сўров"да передатчик ахбороти мавжуд бўлиб, бу ахборот уланишдаги хабар йўқотилишини аниқлашга имкон беради.

Ёлғон уланишни аниқлаш учун ҳар бир чеккадаги "уланишга жавобгар"нинг ҳақиқийлигини ва уланишнинг вақтинчалик яхлитлигини текширишга ишончли асосни таъминловчи қарши чоралар ишлаб чиқилган.

Уланиш бошланиши вақтида ҳар бир чеккада уланишга жавобгарнинг ҳақиқийлигини текшириш кейинги хабарлар оқимининг ҳақикийлиги хусусида қарор қабул қилишга асос ҳисобланади.

Уланишнинг вақтинчалик яхлитлигини текшириш бузғунчининг олдинги қонуний уланиш ёзувидан фойдаланиб, фойдаланувчини хато фикрга солишидан ёки адаштиришидан, маълумотлар узатиш жараёнини бузишидан ҳимоялайди.

XII боб. СИМСИЗ АЛОҚА ТИЗИМЛАРИДА АХБОРОТ ҲИМОЯСИ

12.1. Симсиз тармоқ концепцияси ва тузилмаси

Симсиз тармоқ концепцияси. Симсиз тармоқлар одамларга симли уланишсиз ўзаро боғланишларига имкон беради. Бу силжиш эркинлигини ва уй, шаҳар қисмларидаги ёки дунёнинг олис бурчакларидаги иловалардан фойдаланиш имконини таъминлайди. Симсиз тармоқлар одамларга ўзларига қулай ва хохлаган жойларида электрон почтани олишларига ёки Web-саҳифаларни кўздан кечиришларига имкон беради.

Симсиз тармоқларнинг турли хиллари мавжуд, аммо уларнинг энг муҳим хусусияти боғланишнинг компьютер қурилмалари орасида амалга оширилишидир. Компьютер қурилмаларига шахсий рақамли ёрдамчилар (Personal digital assistance, PDA), ноутбуклар, шахсий компьютерлар, серверлар ва принтерлар тааллуқли. Одатда уяли телефонларни компьютер қурилмалари қаторига киритишмайди, аммо энг янги телефонлар ва ҳатто наушниклар маълум ҳисоблаш имкониятларига ва тармоқ адаптерларига эга. Яқин орада электрон қурилмаларнинг аксарияти симсиз тармоқларга уланиш имкониятини таъминлайди.

Боғланиш таъминланадиган физик худуд ўлчамларига боғлиқ ҳолда симсиз тармоқларнинг қуйидаги категориялари фарқланади:

- симсиз шахсий тармоқ (Wireless personal-area network, PAN);
- симсиз локал тармоқ (Wireless local-area network, LAN);
- симсиз регионал тармоқ (Wireless metropolitan-area network, MAN):
- симсиз глобал тармоқ (Wireless Wide-area network, WAN).

12.1-жадвалда Ушбу тармоқларнинг қисқача тавсифи келтирилган.

Симсиз шахсий тармоқлари узатишнинг катта бўлмаган масофаси билан (17 метргача) ажралиб туради ва катта бўлмаган бинода ишлатилади. Бундай тармоқларнинг характеристикалари ўртача бўлиб, узатиш тезлиги одатда 2Мб/с дан ошмайди.

Бундай тармоқ, масалан, фойдаланувчи PDA сида ва унинг шахсий компьютерида ёки ноутбукида маълумотларни симсиз синхронлашни

таъминлаши мумкин. Худди шу тариқа принтер билан симсиз уланиш таъминланади. Компьютерни ташқи қурилмалар билан уловчи симлар чигалликларининг йўқолиши етарлича жиддий афзаллик бўлиб, бунинг эвазига ташқи қурилмаларнинг бошланғич ўрнатилиши ва кейинги, зарурият туғилганда, жойининг ўзгартирилиши анчагина осонлашади.

12.1-жадвал

Тармоқ хили	Таъсир доираси	Характеристикаси	Стандартлар	Қўлланиш соҳаси
Шахсий симсиз тармоқлар	Фойдаланувчидан бевосита яқинликда	ўртача	Bluetooth, IEEE, 802.15, IRDA	Ташқи қурилмалар кабелларининг ўрнида
Локал симсиз тармоқлар	Бинолар ва кампуслар доирасида	юқори	IEEE 802.15, Wi-Fi, Hiper-LAN	Симли тармоқларни Мобил кенгайтириш
Регионал симсиз тармоқлар	Шахар доирасида	Юқори	Патентли, IEEE 802.16, WIMAX	Бинолар ва корхоналар ва Internet орасида белгиланган симсиз боғланиш
Глобал симсиз тармоқлар	Бутун дунё бўйича	Паст	CDPD ва 2, 2.5 ва 3-авлод уяли телефон орқали тизимлар	Бинодан ташқарида Internetдан мобил фойдаланиш

Симсиз шахсий тармоқларнинг аксарият узатувчи-қабул қилувчиларнинг (transceiver) кам қувват исътемол қилиши ва ихчамлиги микропроцессорлар билан таъминланган, катта бўлмаган фойдаланувчи қурилмаларини самарали мададлашга, ҳамда компьютер қурилмасини узоқ вақт мобайнида битта батареяда (ёки аккумуляторда) ишлашига имкон беради. Ундан ташқари, кам қувват истеъмол қилиниши симсиз шахсий тармоқларни уяли телефонларга, PDA ларга ва наушникларга татбиқ этишга сабаб бўлди.

Симсиз шахсий тармоқлар Internet га ва иловаларга уланишдан биргаликда фойдаланиш мақсадида ноутбуклар ва шахсий компьютерларнинг ўзаро алоқасини таъминлаши мумкин. Бу таъсир доираси битта хона билан чегараланган тармоқларга тўғри келади.

Симсиз локал тармоқлар офисларнинг ичида ва ташқарисида, ишлаб чиқариш биноларида узатишларнинг юқори характеристикаларини таъминлайди. Бундай тармоқлардан фойдаланувчилар одатда ноутбукларни, шахсий компьютерларни ва катта ресурсларни талаб этувчи иловаларни бажаришга қодир процессорли ва катта экранли *PDA* ларни ишлатишади. Хизматчи тармоқ хизматларидан мажлислар залида ёки бинонинг бошқа хоналарида бўла туриб фойдаланаши мумкин. Бу хизматчига ўз вазифаларини самарали бажаришга имкон беради. Симсиз локал тармоқлар узатишнинг 54Мбит/сгача тезлигида барча офис ёки маиший иловалар талабларини қондириш имконига эга. Характеристикалари, компонентлари, нархи ва бажарадиган амаллари бўйича бундай тармоқлар Ethernet хилидаги анъанавий симли локал тармоқларига ўхшаш.

Симсиз регионал тармоқлар юзаси бўйича шахарга тенг бўлган худудга хизмат қилади. Аксарият холларда иловаларни бажаришда белгиланган уланиш талаб этилади, баъзида эса мобиллик зарур бўлади. Масалан, касалхонада бундай тармоқ асосий бино ва масофадаги клиникалар орасида маълумотларни узатишни таъминлайди. Ёки энергетик компания бундай тармоқдан шахар масштабида фойдаланиб, турли туманлардан бериладиган иш нарядларидан фойдаланишини таъминлайди. Натижада, симсиз регионал тармоқлар мавжуд тармоқ инфратузилмаларини бир ерга тўплайди ёки мобил фойдаланувчиларга мавжуд тармоқ инфратузилмалари билан уланишни ўрнатишга имкон беради.

Симсиз Internet хизматлари билан таъминловчилар (Wireless Internet Service Provider, WISP) уйда фойдаланувчилар ва компаниялар учун доимий симсиз уланишларни таъминлаш мақсадида шахарларда ва қишлоқ жойларда симсиз регионал тармоқларни мижозлар ихтиёрига тақдим этади. Бундай тармоқлар, кўпинча симли уланишларни ётқизиш билан боғлиқ чегараланишларга эга бўлган оддий симли уланишларга нисбатан самарали ҳисобланади.

Симсиз регионал тармоқларнинг характеристикалари турлича. Уланишларда инфрақизил технологиянинг ишлатилиши маълумотларни узатиш тезлигининг 100 Гбит/с ва ундан катта бўлишини таъминлайди.

Симсиз глобал тармоқлар мобил иловаларнинг, улардан мамлакат ёки хатто континент масштабида фойдаланишни таъминлаш билан ишланишини таъминлайди. Иқтисодий мулоҳазаларга таянган ҳолда, телекоммуникация компаниялари кўпгина фойдаланувчилар учун узоқ масофадан уланишни таъминловчи симсиз глобал тармоқнинг нисбатан қиммат инфратузилмасини яратадилар. Бундай ечимнинг харажати барча фойдаланувчилар ўртасида тақсимланади, натижада абонент тўлови унчалик юқори бўлмайди.

Кўпгина телекоммуникация компанияларининг кооперацияси туфайли симсиз глобал тармоқларининг таъсир доираси чегараланмаган. Телекоммуникация хизматини таъмнловчиларнинг бирига тўлаб, симсиз глобал тармоқ орқали дунёнинг ҳар қандай нуқтасидан қатор Internet хизматидан фойдаланиш мумкин.

Симсиз глобал тармоқ характеристикалари нисбатан юқори эмас, маълумотларни узатишнинг тезлиги 56 Кбит/с ни, баъзида 170 Кбит/с ни ташкил этади.

Симсиз глобал тармоқларга хос иловалар Internetдан фойдаланишни, электрон почта хабарларини узатиш ва қабул қилишни, фойдаланувчи уйдан ёки офисдан ташқарида бўлганида корпоратив иловалардан фойдаланишни таъминловчи иловалардир. Абонентлар, масалан, таксида кетаётганларида ёки шаҳар бўйича сайр қилинаётганларида уланишни ўрнатишлари мумкин. Умуман, симсиз глобал тармокдан фойдаланувчилар худудий чегараланмаганлар.

Симсиз глобал тармоқлар технологиясини татбиқ этишдаги муаммолардан бири унинг бино ичидаги фойдаланувчилар учун боғланишни таъминлай олмаслиги. Чунки бундай тармоқ инфратузилмалари бино ташқарисида жойлашган ва радиосигналлар бинода айтарлича сусаяди. симсиз глобал тармоқларни бино ичига ўрнатилиши эса қимматга тушади ва техник нуқтаи назаридан асосланмаган.

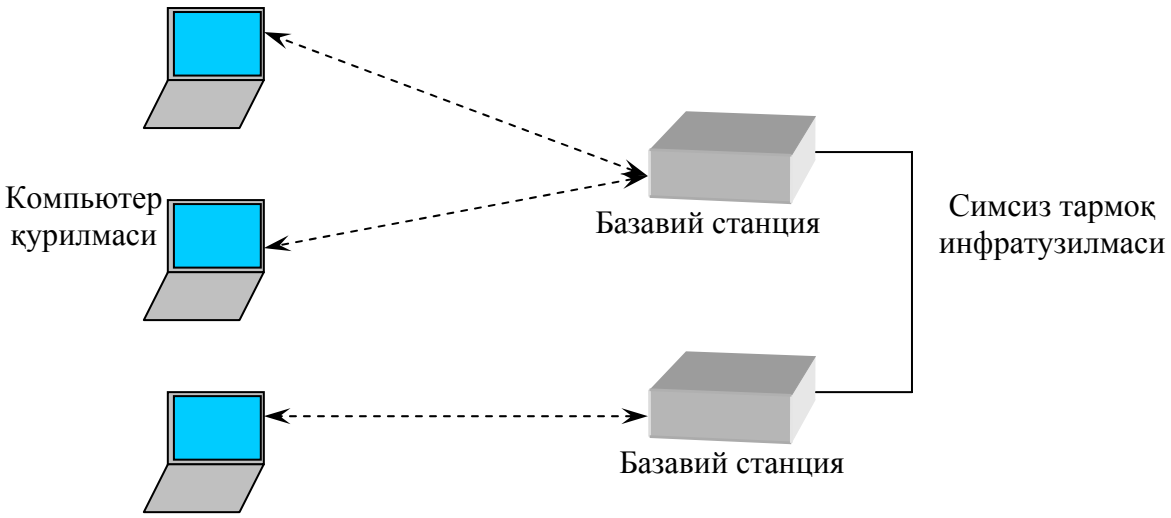
Симсиз шахсий, локал, регионал ва глобал тармоқлар бир-бирини тўлдирувчи бўлиб, турли талабларни қондиради. Аммо, баъзида бир тармоқни иккинчисидан фарқлаб бўлмайди. Масалан, бино ичидаги симсиз локал тармоқ фойдаланувчи PDAси билан шахсий компьютерини симсиз

шахсий тармоқ каби улашни таъминлаши мумкин. Турли симсиз тармоқлар орасидаги фарқни аниқлашда уларда ишлатиладиган технологиялар ва стандартлардан фойдаланишади (12.1-жадвалга қаралсин).

Агар фойдаланувчи нуқтаи назаридан истиқбол хусусида сўз юритилса, симсиз тармоқлар орасида чегаранинг йўқолиши шарт. Турли хил симсиз тармоқ ишини мададловчи компьютер қурилмалари тармоғи интерфейсининг платалари пайдо бўлмоқда. Масалан, сайёхда ёки тижоратчида ҳам симсиз локал ҳам симсиз глобал тармоқ билан ўзаро алоқа қилувчи замонавий уяли телефон бўлиши мумкин.

Симсиз тармоқ тузилмаси. Симсиз тармоқларда симли тармоқда ишлатиладиган компонентлар ишлатилади. Аммо, симсиз тармоқларда ахборот хаво муҳити (medium) орқали узатишга яроқли кўринишга ўзгартирилиши лозим.

12.1-расмда симсиз тармоқларда ишлатиладиган компонентларнинг асосийлари кўрсатилган. Уларга фойдаланувчилар, компьютер қурилмалари, базавий станциялар ва симсиз инфратузилма киради.



12.1-расм. Симсиз тармоқда ишлатиладиган асосий компонентлар

Фойдаланувчилар. Симсиз тармоқ фойдаланувчига хизмат қилишлиги сабабали, фойдаланувчига симсиз тармоқнинг муҳим қисми сифатида қараш мумкин. Фойдаланувчи симсиз тармоқдан фойдаланиш жараёнини бошлайди ва унинг ўзи тугаллайди. Шу сабабли унга "охирги фойдаланувчи" атамаси жоиз ҳисобланади. Одатда, фойдаланувчи симсиз тармоқ билан ўзаро алоқани таъминлаш билан бир қаторда, муайян иловалар билан боғлиқ

бошқа вазифаларни бажарувчи *компьютер қурилмалари (computer device)* билан иш кўради.

Мобиллик - симсиз тармоқнинг энг сезиларли афзалликларидан биридир. Масалан, мобиллик хусусиятидан қандайдир бино бўйича харакатланувчи ва ўзининг PDAси ёрдамида электрон почтани олувчи ёки жўнатувчи одам фойдаланади. Бу ҳолда PDA симсиз тармоқ инфратузилмасига узлуксиз ёки тез-тез тикланувчи уланишни таъминлаши лозим.

Баъзи фойдаланувчиларга фақат компьютер қурилмасининг портативлиги зарур, яъни улар вақтнинг маълум оралиғида симсиз тармоқ билан ишлаганида бир жойда бўладилар. Бундай фойдаланишга мисол тариқасида мажлислар залида симсиз тармоққа уланган ноутбукда ишловчи ходимни кўрсатиш мумкин.

Компьютер қурилмалари. Компьютер қурилмаларининг (баъзида уларни мижозлар деб аташади) кўпгина хиллари симсиз тармоқ билан ишлайолади. Баъзи компьютер қурилмалари фойдаланувчилар учун атайин қурилган бўлса, бошқалари охирги тизим ҳисобланади. 12.2-расмда симсиз тармоқларнинг компьютер қурилмалари келтирилган.

Принтер

Мобил телефон

Ноутбук

Маълумотларни йиғувчи қурилма

Шахсий комьютер

PDA

Оддий телефон

12.2-расм. Симсиз тармоқларнинг компьютер қурилмалари.

Мобил иловалар ишини таъминлаш ва одамларга ўзлари билан узоқ вақт мобайнида олиб юришларида қулайлик туғдириш учун Компьютер қурилмалари ихчам бўлиши лозим. Одатда, улар катта бўлмаган экранга, кам сонли тугмачаларга ва ўлчамлари кичик батареяга эга. Компьютер қурилмалари мобилликка эга бўлга ҳолда фақат баъзи иловаларни мадад-лайди. Нисбатан юқори характеристикаларни талаб этувчи иловаларни ба-жаришда катта экранга ва катта клавиатурага эга бўлган ўлчамлари катта компьютер қурилмаларидан фойдаланилади. Аммо улар массасининг катта-лиги ва бир жойдан иккинчи жойга кўчиришнинг ноқулайлиги муаммо ҳисобланади. Симсиз тармоқларнинг компьютер қурилмалари серверлар, маълумотлар базаси ва Web-узеллар каби охирги тизимларни ҳам ўз ичига олади.

Фойдаланувчилар мавжуд компьютер қурилмаларини симсиз тармоқда ишлатиш учун (масалан, симсиз тармоқ интерфейси платасини ноутбукка ўрнатиш орқали) мослаштиришлари мумкин. *Тармоқ интерфейси платаси* ёки *тармоқ адаптери* (network interface card) компьютер қурилмаси ва симсиз тармоқ инфратузилмаси орасида интерфейсни таъминлайди. Бу пла-та компьютер қурилмаси ичига ўрнатилади, баъзида ташқи тармоқ адаптери ҳам ишлатилади. Бундай адаптерлар, ишга туширилиши билан компьютер қурилмаси ташқарисида қолади.

Компьютер қурилмалари Windows-XP, Linux ёки MAC OS каби опе-рацион тизимга ҳам эга бўлиб, бу операцион тизим симсиз тармоқ илова-ларини амалга ошириш учун зарур бўлган дастурий таъминотни ишга ту-ширади.

Хаво муҳити. Ҳаво компьютер қурилмалари ва симсиз инфратузил-мага орасида ахборот оқимини узатиш канали ҳисобланади. Симсиз тармоқлар орқали алоқани нутқ орқали мулоқотга ўхшатиш мумкин. Агар суҳбатдошлар орасидаги масофа ошаверса, улар бир-бирларини ёмон эшита бошлайдилар.

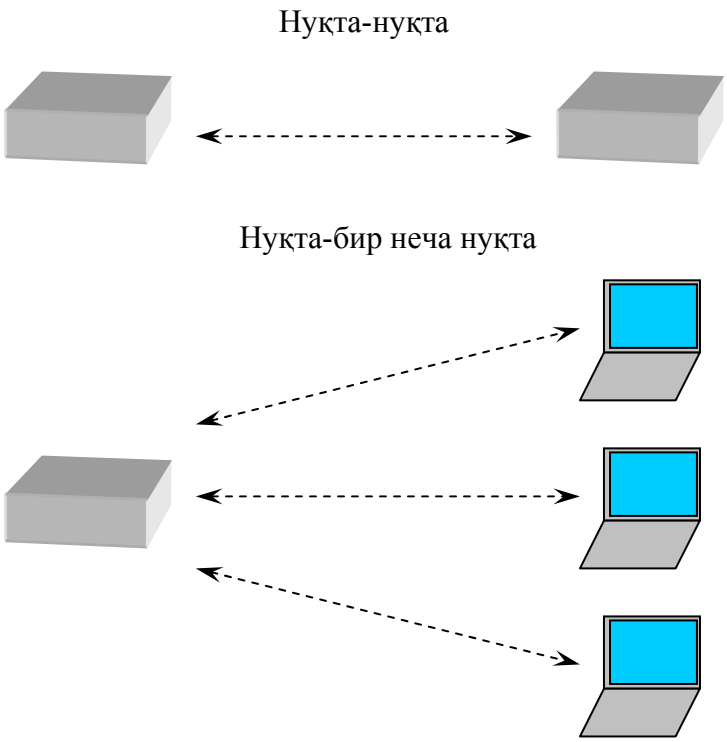
Симсиз тармоқларнинг ахборот сигналлари ҳам хаво орқали тарқалади, аммо ўзининг хусусияти эвазига нутқ сигналарига қараганда ан-чагина катта масофага тарқалиши мумкин. Бу сигналлар одамга эшитил-

майди, шу сабабли уларни, сўзлашга халақит беришидан қўрқмай, янада юқори сатҳларгача кучайтириш мумкин. Аммо алоқа сифати тўсиқларнинг мавжудлигига боғлиқ. Тўсиқлар сигналлар тарқалишига халақит қилади ёки уларни сусайтиради, натижада сигналлар сатҳи пасаяди, уларнинг тарқалиш узоқлиги камаяди.

Ёмғир, қор, туман, тутун (смог) симсиз тармоқларда ахборот сигналларини тарқалишига таъсир этувчи оби-хаво шароитлари ҳисобланади. Масалан, кучли жала алоқа узунлигини икки мартага камайтириши мумкин. Бинолар ва дарахтлар каби бошқа тўсиқлар тарқалиш шароитларига ва симсиз тармоқ характеристикаларига таъсир этиши мумкин. Симсиз регионал ва глобал тармоқларни жойлаштиришни режалаштиришда бу муаммоларнинг муҳимлиги ортади.

Симсиз тармоқлар инфратузилмаси. Симсиз тармоқ инфратузилмаси фойдаланувчилар ва охирги тизимларнинг ўзаро симсиз алоқаларини таъминлайди. Уни базавий станциялар, фойдаланиш контроллерлари, уланиш ўрнатилишини таъминловчи иловаларнинг дастурий таъминоти ва тақсимловчи тизим ташкил этиши мумкин.

Базавий станция инфратузилманинг тарқалган компоненти ҳисобланади. У хаво муҳити орқали тарқалувчи симсиз тармоқ ахборот сигналларининг симли тармоққа узатилишини таъминлайди. Базавий станцияни баъзида *тақсимловчи тизим* деб ҳам юритишади. Демак, базавий станция Web-саҳифаларни кўздан кечириш сервислари, электрон почта ва маълумотлар базаси каби тармоқ хизмати йўналишидан фойдаланишни таъминлайди. Базавий станцияда кўпинча симсиз тармоқ интерфейси платаси бўлиб, бу плата фойдаланувчи компьютеридаги симсиз тармоқ интерфейси платасининг ишлаш принципидан фойдаланади. Базавий станция "нуқта-нуқта" ёки "нуқта-бир неча нуқта" каби уланишларни мададлаши мумкин (12.3-расм).



12.3-расм. Базавий станциянинг "нуқта-нуқта" ва "нуқта-бир неча нуқта" уланишларини мададлаши

"Нуқта-нуқта" тизими сигналлар оқимини бир базавий станциядан иккинчисига ёки бир компьютердан иккинчисига узатиш имкониятига эга. "Нуқта-бир неча нуқта" конфигурацияси холида базавий станция биттадан ортиқ компьютер қурилмаси ёки бир неча базавий станциялар билан боғланиши мумкин. Бундай хил боғланишни, масалан, симсиз локал тармоқ таркибидаги фойдаланиш нуқтаси таъминлайди. Фойдаланиш нуқтаси битта қурилма бўлиб, кўпгина компьютер қурилмалари бир-бирлари билан ҳамда симсиз тармоқ инфратузилмасидаги тизимлар билан боғланиш мақсадида у билан уланишни ўрнатади.

Фойдаланиш контроллери. Фойдаланиш контроллерлари, одатда, тармоқнинг ўтказувчи қисмида, фойдаланиш нуқтаси ва тармоқнинг ҳимояланиш қисми орасида жойлашган аппарат узели ҳисобланади. Фойдаланиш контроллерлари очиқ симсиз тармоқ ва муҳим ресурслар орасида трафикни тартибга солиш мақсадида фойдаланиш нуқталарини марказлаштирилган назоратини таъминлайди. Баъзи холларда фойдаланишни бошқариш вазифасини фойдаланиш нуқтаси бажаради.

Фойдаланиш контроллерлари кенг қўлланилади. Умумфойдаланувчи симсиз локал тармоқда, фойдаланиш контроллери фойдаланувчиларни ау-

тентификациялаш ва авторизациялаш билан Internetдан фойдаланишни тартибга солади.

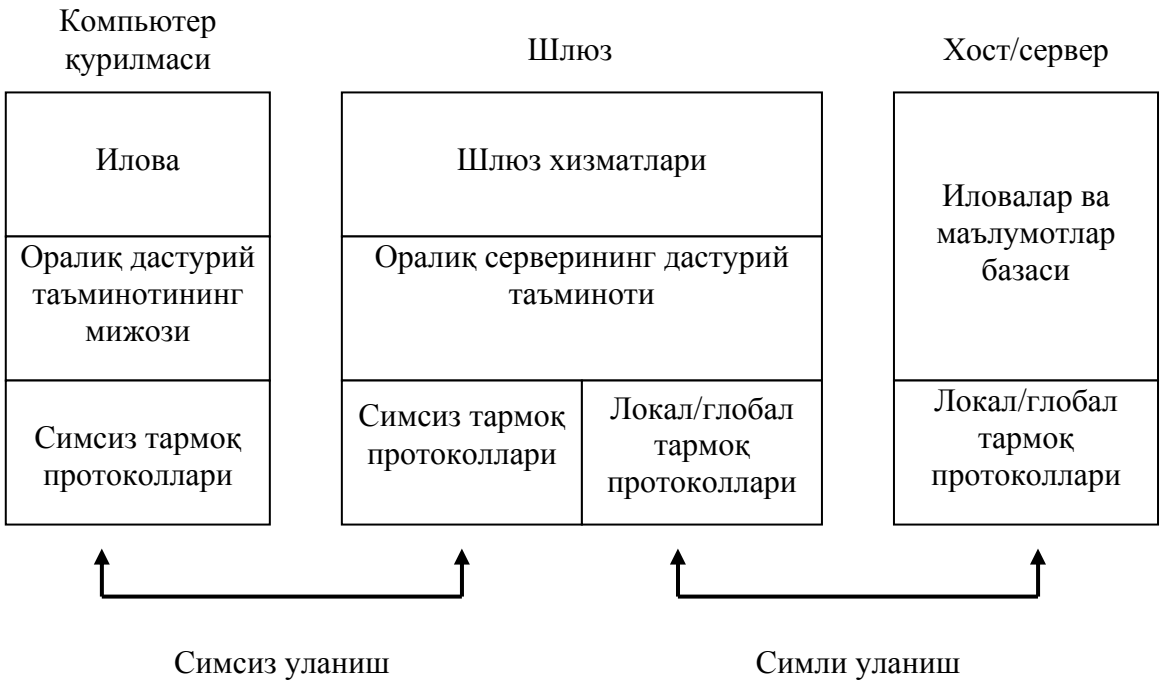
Уланиш ўрнатилишини таъминловчи иловаларнинг дастурий таъминоти. Internet дан ва электрон почтадан симсиз тармоқ орқали, одатда, осон фойдаланилади. Бунинг учун *мижоз қурилмасида* браузер ва электрон почта дастури ўрнатилиши лозим. Фойдаланувчилар вақти-вақти билан симсиз уланишдан маҳрум бўлишлари мумкин, аммо нисбатан мураккаб бўлмаган иловаларни бажаришда ишлатилувчи протоколлар етарлича барқарор ҳисобланади.

Аммо, бундай оддий иловалар билан бир қаторда махсус, янада мураккаб иловалар ишлашини таъминловчи дастурий таъминот зарур. Қуйида уланишни таъминловчи иловаларнинг асосийлари келтирилган.

Терминал эмулятори (therminal emulation). Терминал эмуляторининг дастурий таъминоти компьютер қурилмасида бажарилиб, уни фойдаланувчини нисбатан содда интерфейс билан таъминлашга имкон берувчи терминал каби ишлашга мажбур этади. Бу содда интерфейс фойдаланувчига бошқа компьютерда бажарилувчи иловалар билан ўзаро алоқа қилишга имкон беради.

Маълумотлар базаси билан тўғридан-тўғри уланиш (direct database connectivity). Маълумотлар базаси билан тўғридан-тўғри уланишда (баъзида мижоз-сервер технологияси деб аталади) илова фойдаланувчи компьютерида бажарилади. Бундай конфигурацияда охирги фойдаланувчи қурилмасидаги дастурий таъминот иловага юкланган барча вазифаларни бажаради ва, одатда, марказий серверда жойлашган маълумотлар базаси билан ўзаро алоқада бўлади.

Оралиқ дастурий таъминот (Wireless middleware). Оралиқ дастурий таъминот фойдаланувчининг компьютер қурилмаси ва илова дастурий таъминоти ёки сервердаги маълумотлар базаси орасида оралиқ уланишни амалга оширади (12.4-расм).



12.4-расм. Оралиқ дастурий таъминоти.

Оралиқ дастур симли тармоққа уланган қўшимча компьютерда (оралиқ шлюзида) бажарилади. У фойдаланувчининг компьютер қурилмаси ва серверлар орасида айланувчи пакетларни ишлайди. Бу дастурий таъминот симсиз тармоқда самарали ва ишончли боғланишни яратишга имкон беради, чунки маълумотлар базасига уланиш ва иловаларнинг дастурий таъминоти билан ўзаро алоқа янада ишончли симли тармоқ орқали амалга оширилади. Баъзида бу технологияни чидамли боғланиш (session persistence) деб аташади.

Тақсимланган тизим. Симсиз тармоқ камдан-кам тўла маънода симсиз ишлатилади. Таркибида кўпинча симли уланишлар бўлган тақсимловчи тизим одатда фойдаланиш нуқталарини, фойдаланиш контроллерларини ва серверларни бир бутунга бирлаштириш учун зарур бўлади. Аксарият ҳолларда тақсимловчи вазифасини оддий Internet тармоғи бажаради.

12.2. Симсиз тармоқлар хавфсизлигига таҳдидлар

Симсиз технологиядан фойдаланилиб жуда катта афзалликларга эришиш мумкин. Бу технология фойдаланувчиларга алоқани йўқотмасдан бемалол ҳаракатланиш хиссиётини берса, тармоқ яратувчиларига

боғланишларни ташкил этиш учун катта имкониятларни яратади. Ундан ташқари тармоқдан фойдаланиш учун кўпгина янги қурилмаларни пайдо бўлишига имкон беради. Аммо симсиз технология оддий симли тармоқларга қараганда ўзида кўпроқ таҳдидларни элтади. Хавфсиз симсиз иловани яратиш учун симсиз "хужумлар" ўтувчи бўлиши мумкин бўлган барча йўналишларни аниқлаш лозим. Афсуски, иловалар ҳеч қачон бутунлай хавфсиз бўлмайди, аммо симсиз технологиялардаги хавф-хатарни синчиклаб ўрганиш ҳар холда ҳимояланиш даражасини ошишига ёрдам беради. Демак, мумкин бўлган таҳдидларни тахлиллаб, тармоқни шундай қуриш лозимки, хужумларга халақит бериш ва ностандарт "хужумлар"дан ҳимояланишга тайёр туриш имкони бўлсин.

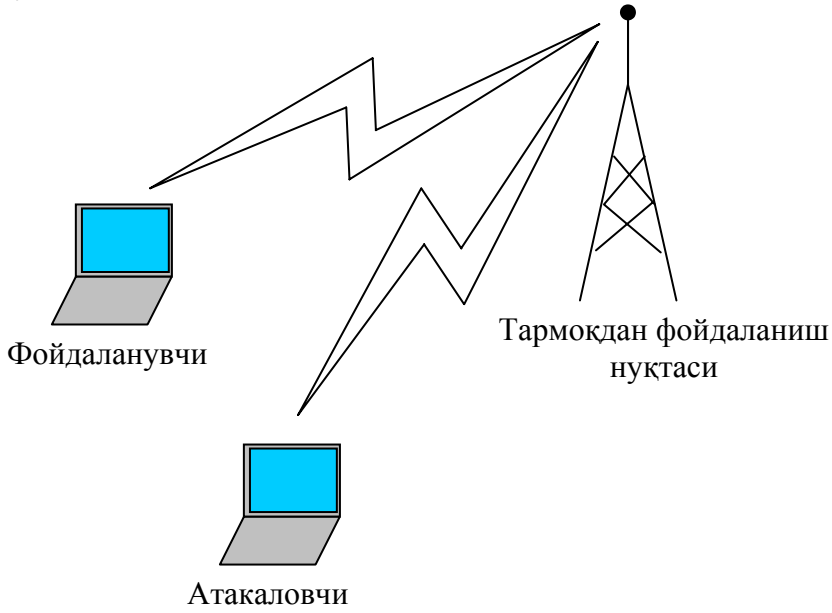
Назоратланмайдиган худуд. Симли ва симсиз тармоқлар орасидаги асосий фарқ тармоқ четки нуқталари орасидаги мутлақо назоратланмайдиган зона билан боғлиқ. Уяли тармоқларнинг етарлича кенг маконида симсиз муҳит асло назоратланмайди. Замонавий симсиз технологиялар тармоқ маконини бошқариш воситаларининг чегараланган тўпламини тақдим этади. Бу симсиз тузилмаларнинг яқинидаги хужум қилувчиларга симли дунёда мумкин бўлмаган хужумларни амалга оширишга имкон беради.

Яширинча эшитиш. Симсиз тармоқлар каби очиқ ва бошқарилмайдиган муҳитда энг тарқалган муаммо – аноним хужумларнинг мумкинлиги. Аноним зараркунандалар 12.5-расмда кўрсатилганидек радиосигналларни ушлаб қолиб, узатилувчи маълумотларни расшифровка қилиши мумкин.

Узатишни ушлаб қолиш учун нияти бузуқ одам узатгич (передатчик) олдида бўлиши лозим. Ушлаб қолишнинг бундай турларини умуман қайдлаш мумкин эмас ва уларга халақит бериш ундан ҳам қийин. Антенналар ва кучайтиргичлардан фойдаланиш, ушлаб қолиш жараёнида нияти бузуқ одамларга нишондан айтарлича узоқ масофада бўлишларига имкон беради.

Яширинча эшитишнинг яна бир усули - симсиз тармоққа уланиш. Локал симсиз тармоқда яширинча фаол эшитиш одатда *Adress Resolution Protocol* (ARP) протоколидан нотўғри фойдаланишга асосланган. Бошида

бу технология тармоқни "эшитиш" мақсадида яратилган эди. Аслида, биз маълумотлар боғланиши сатҳида "man in the middle" (MITM – "ўртада одам", пастроққа қаралсин) хилидаги хужум билан иш кўрамиз. Хужум қилувчи локал симсиз тармоқнинг нишон станциясига сўралмаган ARP-жавобларни юборади, нишон станцияси эса хужум қилувчига ўзидан ўтаётган барча трафикни жўнатади. Сўнгра нияти бузуқ одам пакетларни кўрсатилган адресатларга йўллайди. Шундай қилиб, симсиз станция бошқа симсиз мижознинг (ёки локал тармоқдаги симли мижознинг) трафигини ушлаб қолиши мумкин.

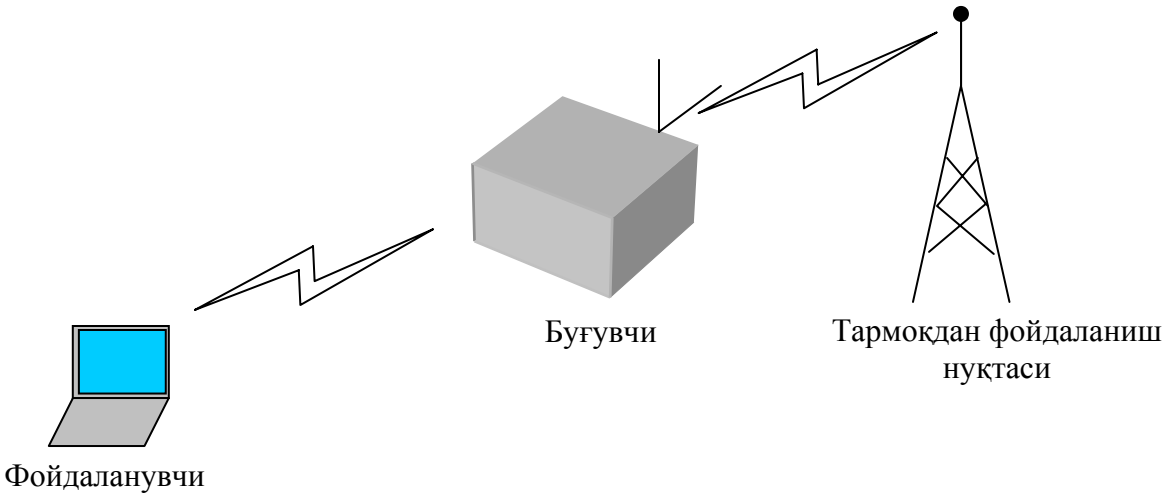


12.5-расм. Симсиз коммуникацияларда яширинча эшитиш

Бўғиш. Тармоқларда бўғиш атайин ёки атайин бўлмаган интерференциянинг алоқа каналидаги жўнатувчи ва қабул қилувчи имкониятидан ошганида содир бўлади. Натижада бу канал ишдан чиқарилади. Хужум қилувчи бўғишнинг турли усулларидан фойдаланиши мумкин.

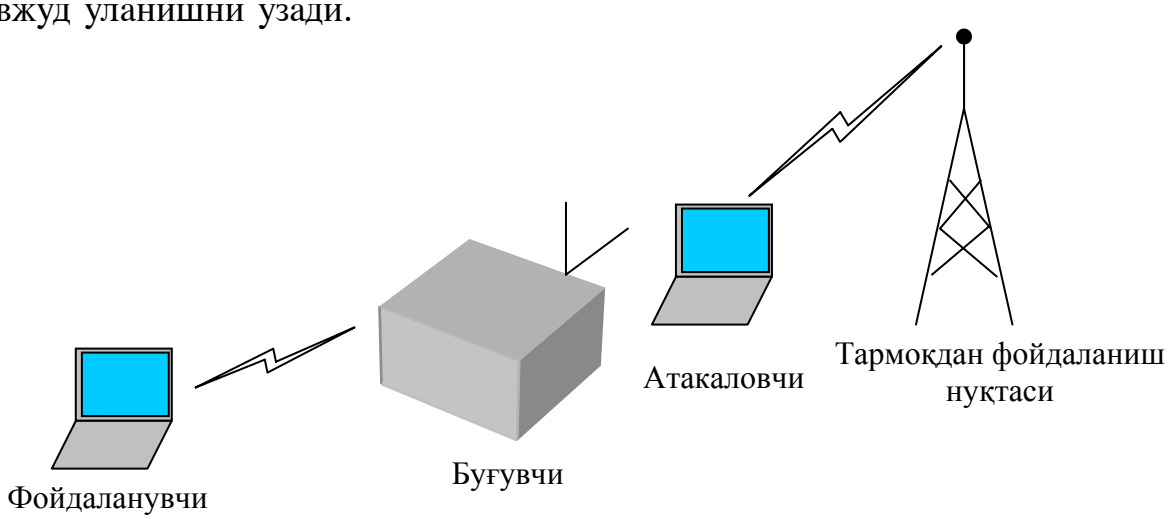
Хизмат кўрсатишдан воз кечиш. DoS (Denial of Service – хизмат кўрсатишдан воз кечиш) хилидаги хужум тармоқни бутунлай ишдан чиқариши мумкин. Бутун тармоқда, жумладан базавий станцияларда ва мижоз терминалларида, шундай кучли интерференция пайдо бўладики, станциялар бир-бирлари билан боғлана олмайдилар (12.6-расм). Бу хужум маълум доирадаги барча коммуникацияни ўчиради. Симсиз тармоққа бўладиган DoS хужумни олдини олиш ёки тухтатиш қийин. Симсиз тармоқ

технологияларининг аксарияти лицензияланмаган частоталардан фойдаланади, демак, бир қанча электрон қурилмалардан интерференция бўлиши мумкин.



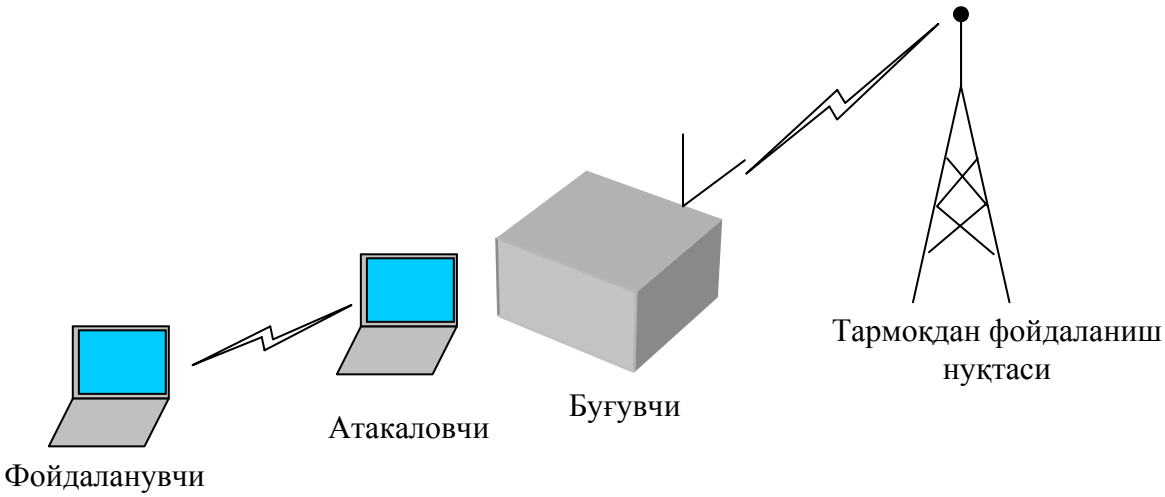
12.6-расм. Симсиз коммуникацияларда буғиш атакалари

Мижозларни бўғиш. Мижоз станциясини бўғиш фирибгарга ўзини бўғилган мижоз ўрнига қўйишига имкон беради (12.7-расм). Мижоз уланишни амалга ошира олмасин деган мақсадда унга хизмат кўрсатишдан воз кечиш учун ҳам буғишдан фойдаланилади. Жуда моҳирлик билан қилинган хужумлар нияти бузуқ одам станциясини базавий станцияга улаш мақсадида мавжуд уланишни узади.



12.7-расм. Уланишни ушлаб қолиш мақсадида мижозни бўғиш атакаси

Базавий станцияни бўғиш. Базавий станцияни бўғиш уни хужум қилувчи станция билан алмаштиришга имкон беради (12.8-расм).



12.8-расм. Уланишни ушлаб қолиш мақсадида базавий станцияни бўғиш атакаси

Бундай бўғиш фойдаланувчиларни хизматлардан фойдаланишдан, телекоммуникация компанияларини эса фойдадан махрум қилади.

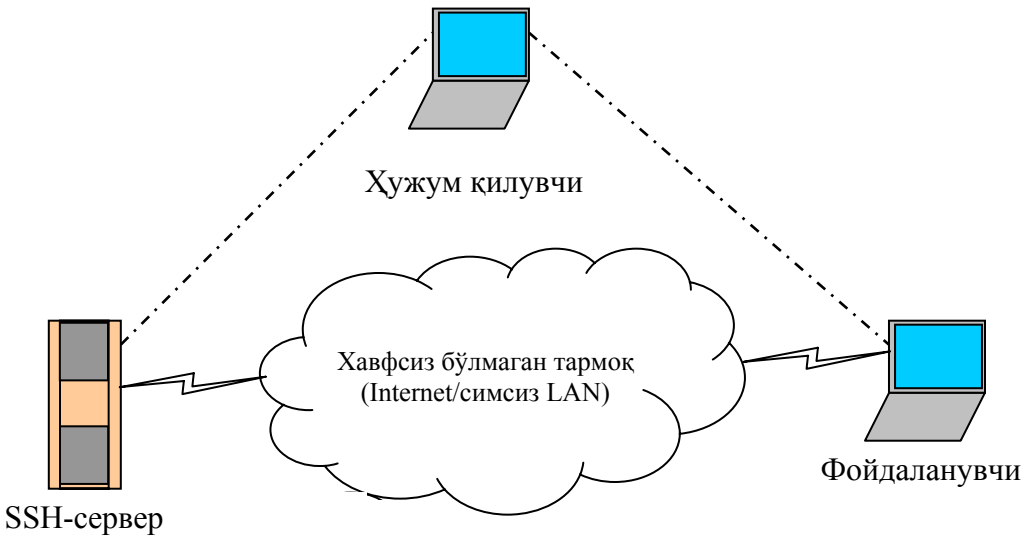
Юқорида қайд этилганидек, аксарият симсиз технологиялар лицензияланмаган частоталардан фойдаланади. Шу сабабли кўпгина қурилмалар – радиотелефонлар, кузатиш тизимлари ва микротўлқинли ўчоқлар – симсиз тармоқ ишига таъсир этиши ва симсиз уланишни бўғиши мумкин. Бундай атайин бўлмаган бўғиш холларини олдини олиш учун, қимматбаҳо симсиз асбоб-ускунани сотиб олишдан аввал у ўрнатиладиган жойни синчиклаб тахлиллаш лозим. Бундай тахлил коммуникацияларга бегона қурилмаларнинг таъсир этмаслигига ишонч ҳосил қилишга имкон беради ва маъносиз харажатлардан асрайди.

Бостириб кириш ва маълумотларни модификациялаш. Нияти бузуқ одам уланишни ушлаб қолиш, маълумотларни ёки командаларни узатиш мақсадида маълумотларнинг мавжуд оқимига ахборотни қўшганида бостириб кириш содир бўлади. Хужум қилувчи пакетларни базавий станцияга юбориб бошқариш командалари ва ахборот оқимлари устида манипуляцияни амалга ошириши мумкин. Бошқариш командаларини керакли бошқариш каналига юбориш орқали фойдаланувчини тармоқдан узишга эришиш мумкин.

Бостириб кириш хизмат кўрсатишдан воз кечиш учун ишлатилиши мумкин. Хужум қилувчи тармоқдан фойдаланиш нуқталарини уланиш командалари билан тўлиб-тоштиради. Натижада бошқа фойдаланувчиларга тармоқдан фойдаланишга рухсат берилмайди.

MITM(man in the middle) хужуми. MITM хужуми юқорида тавсифланган бостириб киришларга ўхшаш. Улар турли шаклларни олишлари мумкин ва алоқа сеансининг конфиденциаллигини ва яхлитлигини бузиш учун ишлатилади. MITM хужумлар анчагина мураккаб, чунки уларни амалга ошириш учун тармоқ хусусида батафсил ахборот талаб этилади. Нияти бузуқ одам, одатда, тармоқ ресурсларидан бирининг идентификациясини бажаради. Хужум қурбони уланишни бошлаганида, фирибгар уни ушлаб қолади ва исталган ресурс билан уланишни тугаллайди, сўнгра ушбу ресурс билан барча уланишларни ўзининг станцияси орқали ўтказади (12.9-расм). Бунда хужум қилувчи ахборотни жўнатиши, жўнатилганини ўзгартириши ёки барча музокараларни яширинча эшитиши ва сўнгра расшифровка қилиши мумкин.

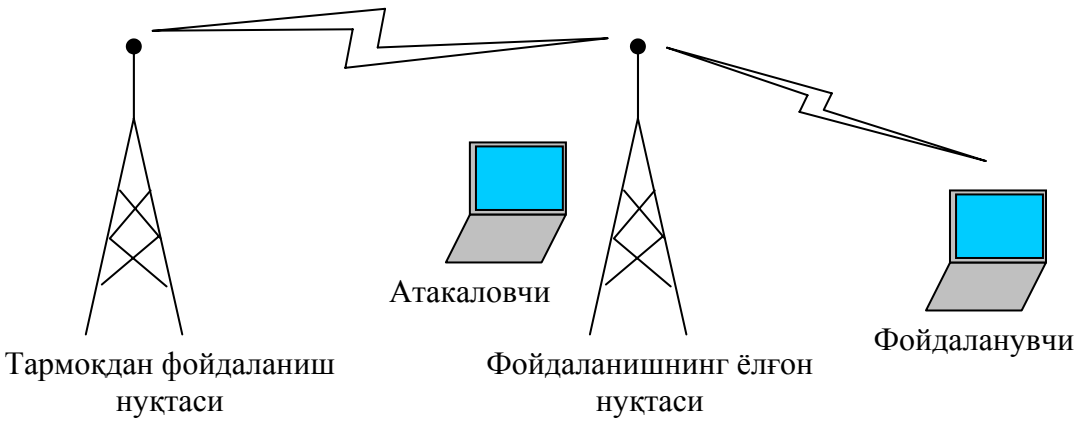
Абонент-фирибгар. Тармоқ абонентининг ишини синчиклаб ўрганиб чиққан хужум қилувчи ўзини "тармоқ абоненти" қилиб кўрсатиб, тармоқ ва унинг хизматларидан фойдаланишга уринади. Ундан ташқари фойдаланишда қўлланиладиган қурилманинг ўғирланиши тармоққа киришга етарли бўлади. Барча симсиз қурилмаларнинг хавфсизлигини таъминлаш осон иш эмас, чунки улар фойдаланувчиларнинг харакатланишида қулайлик туғдириш мақсадида атайин кичкина қилиб яратилади.



12.9-расм. MITM хилидаги атака.

Тармоқдан фойдаланишнинг ёлғон нуқталари. Тажрибали хужум қилувчи тармоқ ресурсларини имитация қилиш билан фойдаланишнинг

ёлғон нуқталарини ташкил этиши мумкин. Абонентлар, хеч шубҳаланмасдан фойдаланишнинг ушбу ёлғон нуқтасига мурожаат этадилар ва уни ўзининг муҳим реквизитларидан, масалан, аутентификация ахборотидан хабардор қиладилар. Хужумнинг бу хили тармоқдан фойдаланишнинг хақиқий нуқтасини "бўғиш" мақсадида баъзида тўғридан-тўғри бўғиш билан биргаликда амалга оширилади (12.10-расм).



12.10-расм. Фойдаланишнинг ёлғон нуқтаси

Симли тармоқдан фойдаланувчилар ҳам, билмасдан тармоқни хужумга очиб бериб фойдаланишнинг ёлғон нуқталарининг ўрнатилишига сабабчи бўлишлари мумкин. Баъзида фойдаланувчи, қулайликка интилиб, симсиз алоқа тақдим этувчи фойдаланишнинг симсиз нуқталарини ўрнатади, аммо хавфсизлик муаммосини ўйламайди. Бу нуқталар симли тармоққа кириш учун "орқа эшик" вазифасини бажариши мумкин, чунки улар турли хужумларга дучор бўладиган конфигурацияда ўрнатилади.

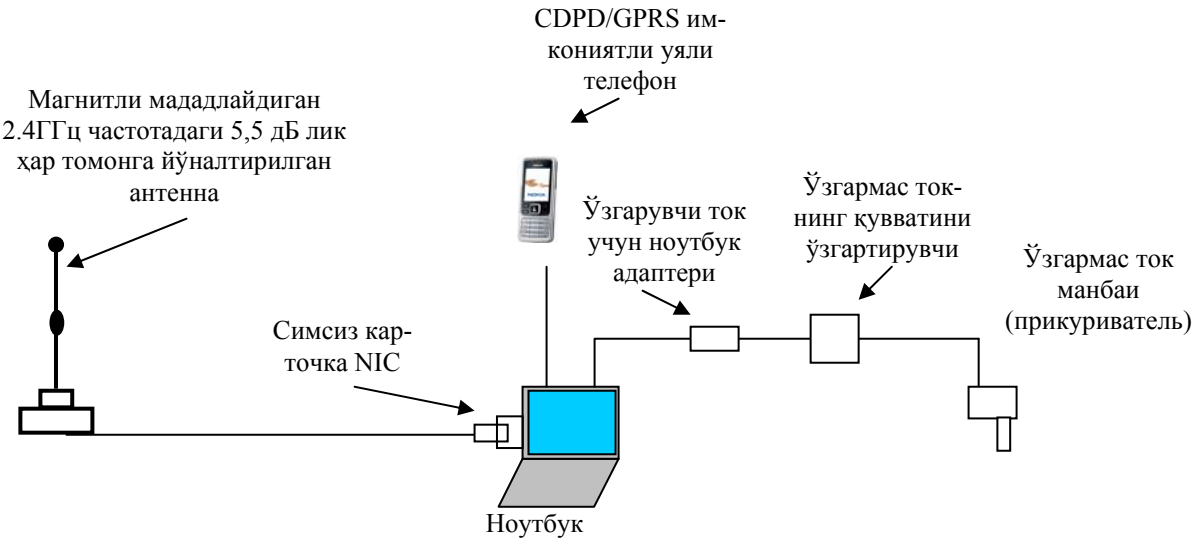
Хужумларнинг анонимлиги. Симсиз фойдаланиш хужумнинг тўлиқ анонимлигини таъминлайди. Ўрнатилган жойни аниқловчи мос тармоқ асбоб-ускунаси бўлмаса, хужум қилувчи анонимликни осонгина сақлаши ва симсиз тармоқ таъсири худудидаги ҳар қандай жойда беркиниши мумкин. Бундай ҳолда нияти бузуқ одамни тутиш қийин, ишни судга ошириш эса ундан ҳам қийин.

Таъкидлаш лозимки, аксарият фирибгарлар тармоқни, уларнинг ички ресурсларига хужум қилиш учун эмас, балки Internetдан текин аноним фойдаланиш учун ўрганадилар ва Internet ҳимоясида бошқа тармоқларни хужумлайдилар.

"Мижоз-мижоз" хилидаги хужумлар. Тармоқнинг барча абонентлари хужумланиши мумкин. Биринчи муваффақиятдан сўнг хужум қилувчи корпоратив ёки телекоммуникацион тармоқдан фойдаланиш хуқуқига эга бўлади. Аксарият тармоқ маъмурлари хавфсизлик режимига талабни оширишга ёки шахсий тармоқлараро экранларни (брандмауэрларни) ўрнатишга етарлича эътибор бермайдилар. Шу сабабли, симсиз тармоқ мижозларига муваффақиятли хужумлар нияти бузуқ одамларга фойдаланувчиларнинг исмини ва паролини очиш, демак, бошқа тармоқ ресурсларидан фойдаланиш имконини бериши мумкин.

Тармоқ асбоб-ускуналарига хужумлар. Нотўғри конфигурацияланган асбоб-ускуналар хужум қилувчилар учун биринчи "хўрак" ҳисобланади ва тармоққа кейинги суқилиб киришга йўл очади. Хужумларнинг асосий объектлари – маршрутизаторлар, узиб-улагичлар, архивларни сақловчи серверлар ва фойдаланиш серверлари.

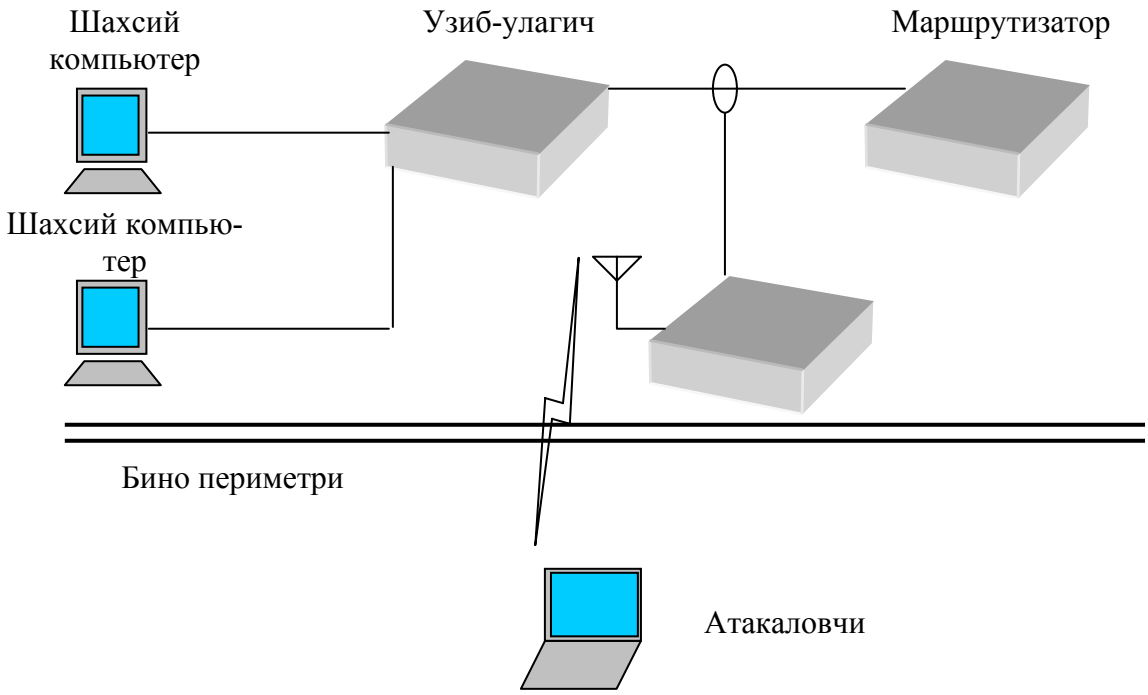
Махфий симсиз каналлар. Симсиз тармоқ фойдаланувчилари тармоқ ни яратиш ёки баҳолаш жараёнида яна бир омилни ҳисобга олишлари зарур. Симсиз фойдаланиш нуқтасининг нархи паст ҳамда дастурий таъминот, стандарт ноутбук ва NIC-карталар асосида фойдаланиш нуқтасини яратиш етарлича осон бўлганлиги сабабли, нокоррект конфигурацияланган ёки симли тармоқда ўйламасдан жойлаштирилган симсиз асбоб-ускунани зийраклик билан кузатиш талаб этилади. Бу асбоб-ускуна (12.11-расм) симли



12.11–расм. "Симсиз урушни" олиб бориш асбоб-ускунаси.

инфратузилмада жуда сезиларли "рахналар" ҳосил қилиши мумкинки, улар тармоқдан бир неча километр узоқдаги хужум қилувчилар диққатини тортиши мумкин.

Худди шунга ўхшаш конструкция ёрдамида ўзига хос "симсиз кўприқ" ўтказиш ва фойдаланиш нуқталарининг бутун занжирини ташкил қилган ҳолда тармоқдан маълумотларни ҳимояланган бино ташқарисида чиқариб олиш мумкин (12.12-расм)



12.12–расм. "Орқа эшик" кўринишидаги тармоқдан фойдаланиш нуқтаси

Роуминг муаммоси. Симсиз тармоқнинг симли тармоқдан яна бир муҳим фарқи фойдаланувчининг тармоқ билан алоқани узмасдан жойини ўзгартириш қобилиятидир. Роуминг концепцияси турли симсиз алоқа стандартлари CDMA (Code Division Multiple Access), GSM (Global System for Mobile Communications) ва симсиз Ethernet учун бир хил. TCP/IPнинг кўпгина тармоқ иловалари сервер ва мижоз IP-адресларининг ўзгармаслигини талаб этади, аммо тармоқдаги роуминг жараёнида абонент албатта унинг бир жойини тарк этиб, бошқа жойига қўшилади. Симсиз тармоқларда мобил IP-адресларнинг ва бошқа роуминг механизмларининг ишлатилиши ушбу талабга асосланган.

Мобил IP-алоқанинг асосий ғояси – фойдаланувчининг турган жойини қайдлаш ва трафикни қайта йўналтириш. Абонент турган жойига боғлиқ бўлмаган адрес TCP/IP – уланишни мададлайди, фойдаланувчи турган жойига боғлиқ бўлган вақтинча адрес эса локал тармоқ ресурслари билан уланишни таъминлайди. IP мобил тизими учун учта тартибга солувчи талаблар мавжуд: мобил узели (фойдаланувчининг симсиз қурилмаси), уй агенти (уй тармоғида жойлашган сервер) ва ажнабий агент (роуминг узатилувчи тармоқда жойлашган сервер). Мобил узели янги тармоққа ўтганида, у турган жойига боғлиқ бўлган вақтинча IP-адресни олади ва ажнабий агентда қайдланади. Сўнгра ажнабий агент уй агенти билан боғланиб мобил агентнинг ўзига боғланганлигини хабар қилади. Шу ондан бошлаб барча пакетлар ажнабий агент-роуминг орқали уй агентига йўналтирилади.

Криптоҳимоялаш таҳдидлари. CDMA, GSM уяли тармоқларда ва симсиз Ethernet-тармоқда ахборотнинг конфиденциаллигини ва яхлитлигини таъминлаш мақсадида криптографик воситалар ишлатилади. Аммо хатоликларга йўл қўйиш коммуникациянинг бузилишига ва ахборотнинг ёмон ниятда ишлатилишига олиб келади.

WEP(Wired Equivalent Privacy – симсиз тармоқ даражасидаги махфийлик) – 802.11 хилидаги тармоқ хавфсизлигини таъминлаш учун яратилган криптографик механизм. WEPни татбиқ этишдаги хатоликлар ва бошқариш муаммолари уни бефойда қилиб қўйди. Ушбу механизм барча фойдаланувчилар ишлатадиган ягона статик калитга эга. Internet тармоқда нияти бузуқ одамга бир неча соат мобайнида калитни тиклашга имкон берувчи воситалар мавжуд. Шу сабабли, WEPга аутентификация ва конфиденциаллик воситаси сифатида ишониш мумкин эмас. Тавсифланган криптографик усулларни ишлатилгани, умуман ишлатилмаганига қараганда яхшироқ, аммо юқорида келтирилган хужумлардан ҳимоялашнинг бошқа усуллари зарур.

12.3. Симсиз тармоқлар хавфсизлиги протоколлари

SSL/TLS протоколлари. Ҳимояланган уланишлар протоколи – Secure Sockets Layer (SSL) Internet браузерларининг хавфсизлиги муаммосини ечиш учун яратилган. SSL таклиф этган биринчи браузер – Netscape Navigator тижорат транзакциялари учун Internet тармоғини хавфсиз қилди, натижада маълумотларни узатиш учун хавфсиз канал пайдо бўлди. SSL протоколи шаффоф, яъни маълумотлар тайинланган жойга шифрлаш ва расшифровка қилиш жараёнида ўзгармасдан келади. Шу сабабли, SSL кўпгина иловалар учун ишлатилиши мумкин.

SSL ўзидан кейинги TLS (Transport Layer Security - транспорт сатҳи ҳимояси протоколи) билан Internetда кенг тарқалган хавфсизлик протоколидир. Netscape компанияси томонидан 1994 йили татбиқ этилган SSL/TLS ҳозирда ҳар бир браузерга ва электрон почтанинг кўпгина дастурларига ўрнатилади. SSL/TLS хавфсизликнинг бошқа протоколлари, масалан, Private Communication Technology (PCT – хусусий коммуникация технологияси), Secure Transport Layer Protocol (STLP-хавфсиз сатҳнинг транспорт протоколи) ва Wireless Transport Layer Security (WTLS – симсиз муҳитда транспорт сатҳини ҳимоялаш протоколи) учун асос вазифасини ўтади.

SSL/TLSнинг асосий вазифаси тармоқ трафигини ёки гипематнни узатиш протоколи HTTPни ҳимоялашдир. SSL/TLS алоқа жараёнининг асосида ётади. Оддий HTTP-коммуникацияларда TCP-уланиш ўрнатилади, хужжат хусусида сўров юборилади, сўнгра хужжатнинг ўзи юборилади.

SSL/TLS уланишларни аутентификациялаш ва шифрлаш учун ишлатилади. Бу жараёнларда симметрик ва асимметрик алгоритмларга асосланган турли технологиялар комбинациялари иштирок этади. SSL/TLSда мижозни ва серверни идентификациялаш мавжуд, аммо аксарият ҳолларда сервер аутентификацияланади.

SSL/TLS турли тармоқ коммуникациялар хавфсизлигини таъминлаши мумкин. Протоколнинг жуда кенг тарқалиши электрон почта, янгиликлар, Telnet ва FTP (File Transfer Protocol – файлларни узатиш протоколи) каби

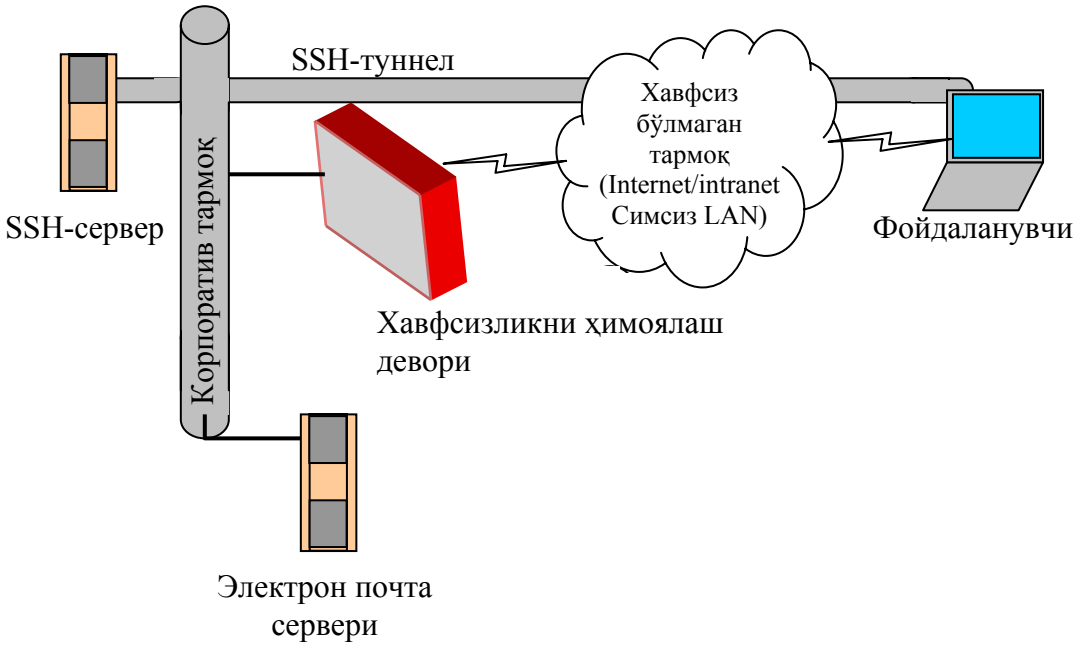
машхур TCP-коммуникациялар билан боғлиқ. Аксарият ҳолларда SSL/TLS ёрдамида коммуникация учун алоҳида портлар ишлатилади.

SSH протоколи. Secure Shell протоколи, SSL/TLSкаби коммуникацияларни ҳимоялаш учун 1995 йили яратилган. Ўзининг мосланувчанлиги ва ишлатилишининг соддалиги туфайли SSH оммавий хавфсизлик протоколига айланди ва ҳозирда аксарият операцион тизимларда стандарт илова ҳисобланади.

SSHда алоқа сеанси жараёнида маълумотларни узатиш учун симметрик калитдан фойдаланилади. Серверни, ҳам мижозни аутентификациялаш учун SSHни осонгина қайта конфигурациялаш мумкин.

Кўпинча SSH тармоқ хостларини бошқаришда ишлатиладиган, кўп тармқалган илова – telnet ни алмаштириш учун ишлатилади.

Баъзида ишлаб чиқарувчилар SSHни telnet ёки FTPни алмаштирувчи сифатида мададламайдилар. Бундай ҳолларда SSHни telnet, FTP, POP (Post Office Protocol - почта хабарлари протоколи) ёки ҳатто HTTP каби хавфсиз бўлмаган иловалар хавфсизлигини таъминлаш учун ишлатиш мумкин. 12.13-расмда трафикни хавфсиз бўлмаган тармоқдан SSH серверга ўтказиш учун конфигурацияланган брандмауэр келтирилган.



12.13–расм. SSH-туннел.

Хавфсиз бўлмаган тармоқдан SSH серверга ва аксинча ҳеч қандай трафик ўтказилмайди. SSH-сервернинг SSH дан терминал фойдаланишидан ташқари, портнинг қайта йўналтирилиши электрон почта трафигини SSH-серверга хавфсиз тармоқ бўйича узатилишини таъминлаши мумкин. Сўнгра SSH-сервер пакетларни электрон почта серверига қайта йўналтиради. Электрон почта серверига трафик SSH-сервердан келганидек туюлади ва пакетлар SSH-серверга, фойдаланувчига туннеллаш учун юборилади.

WLTS протоколи. SSL/TLSга асосланган WLTS протоколи WAP (Wireless Application Protocol – симсиз иловалар протоколи) қурилмаларида, масалан, уяли телефонларда ва чўнтак компьютерларида ишлатилади. SSL ва WLTS бир-биридан транспорт сатҳи билан фарқланади. SSL йўқолган пакетларни қайта узатишда ёки ностандарт пакетларни узатишда TCP ишига ишонади. WLTSдан фойдаланувчи WAP қурилмалари ўз функцияларини бажаришида TCPни қўллай олмайдилар, чунки фақат UDP (user Datagram Protocol) бўйича ишлайдилар. UDP протоколи эса уланишга мўлжалланмаган, шу сабабли бу функциялар WLTSга киритилиши лозим.

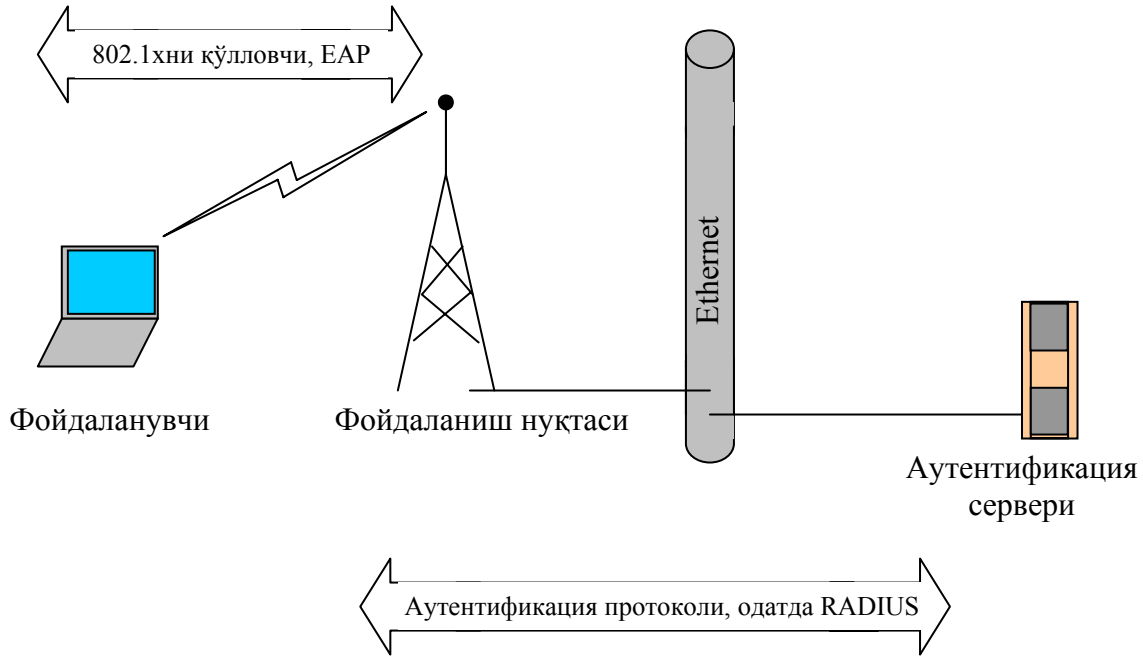
"Қўл бериб кўришиш" жараёнида қуйидаги учта синф фаоллашиши мумкин:

- WLTS – 1-синф. Сертификатсиз;
- WLTS – 2-синф. Сертифкатлар серверда;
- WLTS – 3-синф. Сертифкатлар серверда ва мижозда.

1-синфда аутентификациялаш бажарилмайди, протокол эса шифрланган канални ташкил этишда ишлатилади. 2-синфда мижоз (одатда фойдаланувчи терминал) серверни аутентификациялайди, аксарият ҳолларда сертификатлар терминалнинг дастурий таъминотига киритилади. 3-синфда мижоз ва сервер аутентификацияланади.

802.1x протоколи. Бу протоколнинг асосий вазифаси - аутентификациялашдир; баъзи ҳолларда протоколдан шифрловчи калитларни ўрнатишда фойдаланиш мумкин. Уланиш ўрнатилганидан сўнг ундан фақат 802.1x. трафиги ўтади, яъни DHCP (Dynamic Host Configuration Protocol - хостларни динамик конфигурациялаш протоколи), IP ва ҳ. каби протоколларга

рухсат берилмайди. Extensible Authentification Protocol (EAP) (RFC 2284) фойдаланувчиларни аутентификациялашда ишлатилади. Бошланишида EAP "нуқта-нуқта" (PPP, Point-to-Point Protocol) пртоколи ёрдамида аутентификациялашнинг баъзи муаммоларини ҳал этиш учун ишлаб чиқилган эди, аммо унинг асосий вазифаси симсиз алоқа муаммоларини ҳал этишга қаратилиши лозим. EAPнинг аутентифкациялаш пакетлари фойдаланувчи маълумотларини киритган фойдаланиш нуқтасига юборилади; аксарият ҳолларда бу маълумотлар фойдаланувчи исми (login) ва паролдан иборат бўлади. Фойдаланиш нуқтаси тармоқ яратувчиси танлаган воситаларнинг бири билан фойдаланувчини идентификациялаши мумкин. Фойдаланувчи идентификацияланганидан ва шифрлаш учун канал ўрнатилганидан сўнг алоқа мумкин бўлади ва DHCP каби протоколларнинг ўтишига рухсат берилади (12.14-расм).

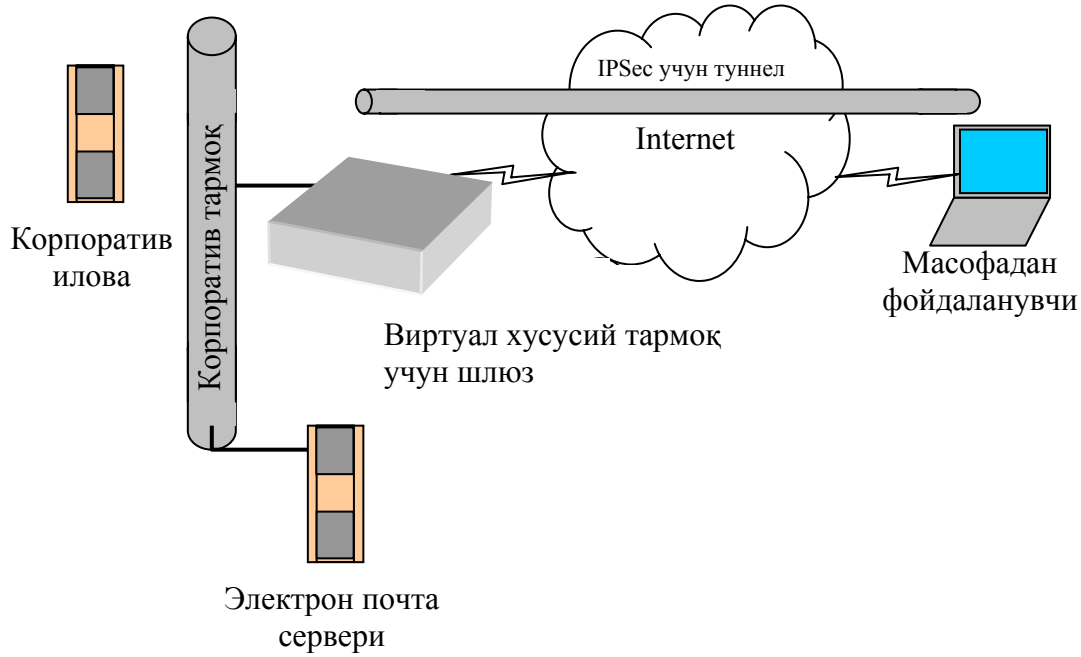


12.14–расм. 802.1x протоколининг кўриниши

IPSec протоколи. Протоколлар стекида IPSec протоколи SSL/TLS, SSH ёки WLTS протоколларидан пастда жойлашган. Хавфсизликни таъминлаш IP-сатҳида ва Internet-моделда амалга оширилади. IPSec ни татбиқ қилиш усулларидан кўп тарқалгани туннеллаш бўлиб, у битта сессияда IP-трафикни шифрлаш ва аутентификациялаш имконини беради. IPSec ҳозирда Internetда ишлатилувчи аксарият виртуал хусусий

тармоқлардаги (VPN-Virtual Private Network) асосий технология ҳисобланади. IPSecнинг мослашувчанлиги ва иловалар танланишининг кенглиги сабабли, кўпчилик айнан бу схемадан симсиз иловалар хавфсизлигини таъминлашда фойдаланади.

IPSecни иловаларга асосланган қўлланишининг жуда кўп имкониятлари мавжуд. Хавфсиз коммуникациялар учун IPSecнинг қўлланиши кўпинча Internet орқали масофадан фойдаланиш виртуал хусусий тармоғи VPN билан боғлиқ. Қачонки умумфойдаланувчи тармоқ хусусий тармоқ функцияларини амалга ошириш учун ишлатилса, уни VPN деб аташ мумкин. Бундай таърифга ATM (Asynchronous Transfer Mode - узатишнинг асинхрон усули), Frame Relay ва X.25 каби тармоқ технологиялари ҳам тушади, аммо аксарият одамлар Internet бўйича шифрланган канални ташкил этиш хусусида гап кетганида VPNатамасини ишлатишади. Корпоратив тармоқ периметри бўйича 12.15-расмда кўрсатилганидек шлюзлар ўрнатилади ва IPSec-туннел орқали шлюздан масофадан фойдаланиш амалга оширилади.



12.15–расм. IPSec VPN-туннел.

12.4. Симсиз қурилмалар хавфсизлиги муаммолари

Симсиз қурилмаларни тўртта категорияга ажратиш мумкин: ноутбуклар, чўнтак компьютерлари (PDA), симсиз инфратузилма (кўприклар, фойдаланиш нуқталари ва ҳ.) ва уяли телефонлар.

Ноутбуклар – корпоратив симсиз тармоқларда ва SOHO (Small Office Home Office – кичик ва уй офислари) тармоқларида кенг тарқалган қурилма.

Физик хавфсизлик ноутбуклар учун жиддий муаммо ҳисобланади. Бундай компьютерларни харид қилишдаги параметрлардан бири-унинг ўлчами. Ноутбук қанчалик кичкина бўлса, у шунчалик қиммат туради. Бошқа тарафдан, ноутбук қанчалик кичкина бўлса, уни ўғирлаш шунчалик осонлашади. Шифрлаш калитларининг, масалан, WEP-калитлар (Wired Equivalent Privacy), дастурий калитлар, пароллар ёки шахсий калитларнинг (PGP, Pretty Good Privace кабилар) йўқотилиши катта муаммо ҳисобланади ва уни иловалар яратилиши босқичидаёқ ҳисобга олиш зарур. Нияти бузуқ одам ноутбукни ўз ихтиёрига олганидан сўнг аксарият хавфсизлик механизмлари бузилиши мумкин.

Ноутбукларнинг мобиллилиги уларнинг корпоратив тармоқлараро экранлар (брандмауэрлар) билан ҳимояланмаган бошқа тармоқлар билан уланиш эҳтимоллигини оширади. Бу Internet-уланишлар, фойдаланувчи тармоқлар, асбоб-ускуна ишлаб чиқарувчиларининг тармоғи ёки рақиблар ҳам жойланувчи меҳмонхона ёки кўргазмалардаги умумфойдаланувчи тармоқлар бўлиши мумкин. Бундай ҳолларда мобил компьютерларнинг ахборот хавфсизлиги хусусида жиддий ўйланиш лозим.

Ноутбукларнинг физик сақланишларини таъминлаш усулларидан бири-хавфсизлик кабелидан фойдаланиш. Ушбу кабел ноутбукни столга ёки бошқа йирик предметга "бойлаб" қўйишга мўлжалланган. Албатта, бу юз фоизлик кафолатни бермайди, аммо ҳар холда ўғрининг анчагина куч сарф қилишига тўғри келади.

Ноутбукларнинг тез-тез ўғирланиши сабабли, ахборотни архивлашнинг хавфсизликни таъминлашга нисбатан муҳимлиги кам эмас. Шифрлаш

дастурлари файллар хавфсизлигини таъминлашда ёки қаттиқ дискларда шифрланган маълумотлар хажмини яратишда ишлатилади. Бу маълумотларни расшифровка қилиш учун, одатда, паролни киритиш ёки шахсий калитларни ишлатиш талаб этилади. Барча ахборотларни шифрланган файлларда ёки архивларда сақланиши керакли файллар тўпламини архив учун нусхалашни енгиллаштиради, чунки улар энди маълум жойда жойлашган бўлади.

Ўғрилар учун ноутбуклар "биринчи номерли нишон" эканлигини фойдаланувчилар тушуниб етишлари ва уларни қаровсиз қолдирмасликлари зарур. Ҳатто офисларда ноутбукни кечага қолдириш мумкин эмас, чунки офисга кўп кишилар (компания ходимлари, фаррошлар, мижозлар) ташриф буюрадилар.

Ахборотнинг чиқиб кетиши ноутбук эгасининг кўп одамлар тўпланган жойларда ҳам содир бўлиши мумкин. Самолет – компания менеджерлари фойдаланадиган одатдаги транспорт воситасидир. Самолетда қўшни креслодаги йўловчи ноутбук эгасининг елкаси устидан муҳим ахборотни ўқиб олиши мумкин. Ҳатто "уй шароитидаги" ноутбуклар ҳам ҳимояланиши зарур. Бу ҳолда компьютернинг ҳимояси сервер ҳимоясидан фарқланмайди. Жуда ҳам зарур бўлмаган сервисларнинг ўчирилиши қурилма ишлашини яхшилайди.

Ўзининг дастурий таъминотини ноутбукка ўрнатган нияти бузуқ одам хавфсизликнинг барча механизмларини четлаб ўтиш имкониятига эга бўлади. Компьютерни ўз ихтиёрига олган ўғри унга ўзининг дастурини ўрнатганида уни тухтатиб бўлмайди. BIOSда (Basic Input/Output System-киритиш/чиқаришнинг базавий тизими) ва қаттиқ дискда ўрнатилган пароллар ўғриланган ноутбукдан фойдаланишга тўсқинлик қилиши мумкин.

Ушбу барча воситалар, афсуски, тажрибали хакер учун тўсиқ бўлаолмайди.

Чўнтак компьютерлари. PDA(Personal Digital Assistans – "шахсий рақамли ёрдамчилар")нинг кўпгина хилларидан симсиз иловалар билан ишлашда фойдаланилади. Махсус қурилган PDAларда тиббиёт, саноат ёки авиация иловалари ишга туширилади. Чўнтак компьютерлари ҳам мавжуд бўлиб, уларда симсиз алоқа учун ўрнатилган карточка, штрих кодларнинг

сканери, хизмат муддати узоқ бўлган батареялар ёки магнит ҳошияли карталарни ўқувчи қурилма каби қўшимча қурилмалар билан биргаликда Palm OS ёки Windows SE операцион тизим ўрнатилган. Бундай компьютерлардан фойдаланиш учун махсус техник тайёргарлик талаб этилмайди. Шунга ўхшаш қурилмаларни ёки иловаларни ҳимоялаш айниқса мураккаб масала ҳисобланади.

PDAдан фойдаланишга хоҳиш билдирган хужум қилувчи учун ундаги ахборот киритиш механизмларининг барчаси нишон ҳисобланади. Ундан ташқари, аксарият чўнтак компьютерлари шундай ишлаб чиқилганки, уларни ишлаб чиқувчилари учун иловалардаги хатоликларни осонгина аниқлаш йўллари таъминланган. Хатоликларни аниқлашда ишлатилувчи интерфейслар нияти бузуқ одамлар учун ҳақиқий "тешик" хизматини ўташи мумкин.

Чўнтак компьютери ишлайдиган ахборотни ҳимоялаш учун ахборотни чўнтак компьютерида эмас, балки маълумотларнинг хавфсиз резерв базасида сақлаш лозим. Яна бир вариант – JAVA тили иловасидан ёки фойдаланувчи учун махсус яратилган иловалардан фойдаланиш. Бу ҳолда ахборот қурилмада сақланмайди, аммо, PDAнинг дисплейида акслантирилади. Бошқача айтганда, симсиз иловалардан фақат симсиз тармоқдан фойдаланиш мавжуд бўлган жойларда фойдаланиш мумкин.

Аксарият PDAларда парол ёрдамида блокировка ва разблокировка қилиш имконияти мавжуд. Бу усулларга бутунлай ишонмаслик лозим, аммо улар нияти бузуқ одамларни вақтинча тухтатиб туриши мумкин. Ундан ташқари PDAни блокировка қилиш тизими қурилмадаги иловалардан ёки ахборотдан нияти бузуқ одамларнинг фойдаланишни қийинлаштиради. PDAнинг зарур бўлмаган барча функцияларини ўчириб қуйиш лозим, чунки ҳар бир ўчирилган киритиш механизми бўлиши мумкин бўлган хужумлар сонини камайтиради.

Чўнтак компьютерида муҳим ахборотни сақлаш учун шифрлашни қўллаш ва унга қўшимча сифатида манбани улаш ва экранни блокировка қилиш учун пароллар ўрнатиш тавсия этилади.

Симсиз инфратузилма. Симсиз инфратузилма қурилмалари одатда одамлар йиғилган ерда жойлаштирилади. Уларга кафелар, аэропортлар,

корпоратив тадбирларни ўтказиш жойлари ва ҳ. киради. Турли хил одамлар EAP(Extensible Authentification Protocol – аутентифкациялашнинг кенгайтирилувчи протоколи) ёки WEP каби хавфсизлик воситаларини ишдан чиқариш ёки тармоққа суқилиб кириш учун тармоқ конфигурацияси хусусидаги ахборотни қўлга киритиш мақсадида ушбу компонентлардан фойдаланишни хохлашлари мумкин.

Симсиз инфратузилма қурилмаларида тармоқни бошқариш функцияларининг хавфсизлигини таъминлаш учун улардан фойдаланишда SSH, SSL (Secure Sockets Layer) ёки SNMP3 (Simple Network Management Protocol 3 – тармоқни оддий бошқариш протоколи, 3-версия) каби хавфсиз протоколлардан фойдаланиш лозим. Ундан ташқари telnet, HTTP даги тўғри матн, ва SNMP (биринчи версия) каби хавфсизлик етарли даражасини мададламайдиган протоколлар ўчирилиши лозим. Хавфсиз бошқаришни таъминлаш иложи бўлмаса, фойдаланишнинг баъзи бир нуқталарини кетма-кет портлар орқали бошқариш мантиқан тўғри ҳисобланади. Фойдаланиш нуқталарини юқорига қўл етмайдиган жойга маҳкамлаб қўйиш ҳам уларни ўғирланишдан сақлайди.

Уяли телефонлар. Уяли телефонлар учун хавфсизлик мулохазалари ноутбук ва PDAларга нисбатан келтирилган мулоҳазаларга ўхшаш. Қурилмаларнинг ўзи ва мос дастурий таъминот учун хавфсизлик муаммоси ҳам ҳеч нимаси билан фарқ қилмайди.

Уяли телефонлар ҳам бошқа симсиз қурилмаларга бўладиган хужумларга дучор бўладилар. Одатда буфернинг тўлиб-тошиши, қатор форматига хужумлаш, грамматик хатоликлар ишлатилади, натижада хужум қилувчи ўғирланган қурилмада ўзининг дастурини ишга туширишга эришади. Мисол сифатида SMSнинг қисқа хабарларини кўрсатиш мумкин. Ўзининг телефони орқали SMS жўнатган фойдаланувчига хужумга дучор бўлиши хавфи туғилади. Бу хужум натижасида хизмат қилиш тўхтатилади ёки фойдаланувчи терминалида бегонанинг командалари бажарилади.

Ундан ташқари SIM-карталарни (Subscriber Idenity Module – абонент идентифкацияси модули) ишлаб чиқарувчилари қурилмаларига уяли телефонга симсиз интерфейс орқали юкланилиши рухсат этиладиган қўшимча

функцияларни кирита бошладилар. Мисол тариқасида Sim Toolkit ва МЕХЕни кўрсатиш мумкин. Зарарли иловаларни бошқа фойдаланувчига узатишни олдини олувчи усуллар ташқи хужумларга дучор бўлади. Бундай иловаларнинг моҳияти шундаки у нияти бузуқ одамга фойданувчининг адрес китобини ёки телефондаги бутун SMS рўйхатини узатиши мумкин. Баъзи ечимлар DES стандарти асосида ишлайди, аммо худди шундай DES-калитлар ҳар бир SIM-карталар учун ишлатилади.

Терминаллар учун парол ёки PIN-кодларни ишлатиш тавсия этилади. GSM(Global System for Mobile Communications – мобил коммуникацияларнинг глобал тизими) тармоқларида ишловчи телефонлар хавфсизлигини таъминлашда SIM PIN керак бўлади. Бу функциядан максимал фойдаланиш учун барча бўлиши мумкин бўлган PINлардан фойдаланиш ҳамда IMEI (International Mobile Equipment Identity – мобил қурилманинг ҳарқаро номери)нинг ишончли жойда ёзилиши тавсия этилади.

Муҳим ахборотни узатиш учун терминалдан фойдаланишида ахборотни албатта шифрлаш зарур. Кредит карточкалар номерларини ёки бошқа шахсий ахборотни узатиш учун албатта SSL-ҳимояли WTLS-уланиш хизматидан фойдаланиш зарур. Ундан ташқари GSM ичидаги алгоритмларга бўладиган аксарият хужумлар нияти бузуқ одамга фойдаланувчининг телефон номерини ўйлаб чиқаришга (клонировка) имкон беради. Бу хужумлар одатда телефон мавжудлигини талаб қилади, шу сабабли телефонни хавфсиз жойда сақлаш, йўқотилган ёки ўғирланган ҳолда тезлик билан операторга хабар бериш лозим.

XIII боб. ХАВФСИЗЛИКНИ БОШҚАРИШ ВА ҲИМОЯ ТИЗИМИНИ ҚУРИШ

13.1. Бошқаришнинг функционал масалалари

Замонавий ахборот технологияларидан муваффақиятли фойдаланиш учун нафақат тармоқларнинг ўзини, балки тармоқ хавфсизлиги воситаларини ҳам ишончли ва самарали бошқариш зарур. Ҳозирги вақтда компаниянинг бутун инфратузилмасини қамраб олувчи бошқаришнинг комплекс тизимини яратиш биринчи галдаги вазифа ҳисобланади. Бундай бошқариш тизими ахборот тизимининг мураккаблиги ва масштабидан қатъий назар, қуйидагиларга имкон яратади:

- бутун ахборот инфратузилмасига марказлаштирилган ва оператив бошқариш таъсирни кўрсатиш;

- оператив ечимларни қабул қилиш учун ахборот хавфсизлиги ҳолати хусусидаги объектив ахборотни берувчи мунтазам аудитни ва кенг кўламдаги мониторинг ўтказиш;

- ахборот инфратузилмаси ривожини башоратлаш учун унинг ишлаши хусусидаги статистик маълумотларни тўплаш.

Ахборот тизимларини бошқаришнинг ITIL методологияси

ITIL (IT Infrasructure Library) методологиясига мувофиқ ахборот тизими иккита йирик блокдан – ахборот инфратузилмаси ва ахборот сервисларидан иборат (13.1-расм).

13.1–расм. ITIL методологияси нуқтаи назаридан ахборот тизимининг кўриниши

Ахборот инфратузилмаси ахборот сервислари ишловчи моддий асос, муҳит ҳисобланади. Ахборот сервисларига Internet-сервислар, иловалар сервиси, бошқариш, ечим қабул қилиш сервислари ва ҳ. киради. Ахборот инфратузилмаси сервислар ишлашини таъминловчи техник воситалар, алоқа линиялари, муолажалар, меъёрий хужжатлар ва ҳ. мажмуидир. Ахборот сервисларининг сифати бевосита ахборот инфратузилмаси ва уни бошқариш сифатига боғлиқ.

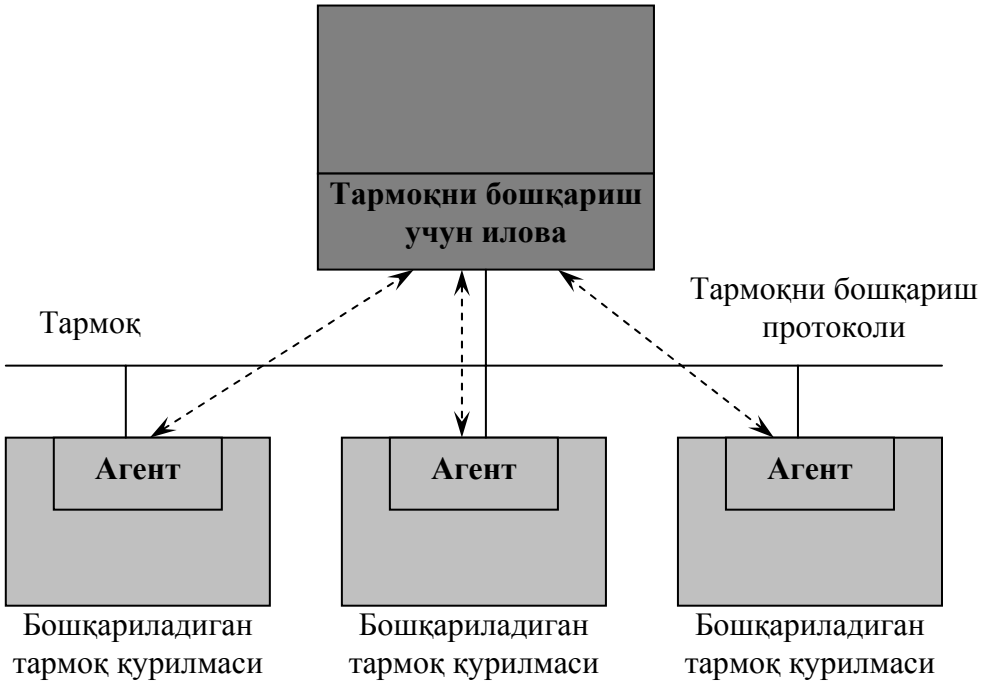
Ахборот инфратузилмасини асосида ахборот ресурслари (ҳисоблаш платформалари, серверлар, шахсий компьютерлар, маълумотларни узатиш тармоқлари, алоқа линиялари) ётувчи пирамида сифатида тасаввур этиш мумкин (13.2-расм).

13.2–расм. Ахборот инфратузилмасини ташкил этувчилари

Пирамиданинг иккинчи сатҳини турли иловалар ташкил этади. Бу иловалар биринчи сатҳ ресурсларидан фойдаланиб татбиқий дастур таъминоти, электрон почта, кафолатланган етказиш тизими, маълумотлар базаси, Web-серверлар ва ҳ. каби муайян иловалар ишлашини таъминлайди. Ва ниҳоят, энг юқори сатҳда бизнес ва ишлаб-чиқариш жараёнларининг ўтишини таъминловчи иловалар ишлайди. Иккала пастки сатҳдан фойдаланувчи бу иловалар ишлаб-чиқаришни бошқариш, буюртмачилар ва таъмин-

ловчи билан ўзаро алоқа, молиявий ҳисоб ва ечимни қабул қилишни мададлаш каби бизнес масалаларни ечишга йўналтирилган.

Умумий ҳолда, тармоқни бошқариш тизимининг архитектураси 13.3-расмда келтирилган кўринишга эга. Тармоқни бошқариш иловаси тармоқ маъмурининг иш жойида ёки бошқа компьютерда бажарилиши мумкин. Унинг вазифаси бошқарилувчи қурилмаларда бажариладиган *агент* - иловалардан ёки операцион тизим сервисларидан келувчи бошқарилувчи объект хусусидаги ахборотни йиғиш.



13.3–расм. Тармоқни бошқариш тизимининг умумлаштирилган архитектураси

Бундай иловаларни агентлар билан ўзаро алоқаси учун одатда SNMP (Simple Network Management Protocol) ёки CMIP (Common Management Information Protocol) протоколларидан фойдаланилади. Биринчиси, одатда, локал тармоқда ишлатилса, иккинчиси телекоммуникациядан фойдаланувчи тақсимланган тармоқларда ишлатилади. Аммо дастур таъминотини баъзи ишлаб чиқарувчилари тармоқни бошқаришда хусусий тармоқ протоколларидан фойдаланишади.

Тармоқни бошқарувчи замонавий воситалар қуйидаги вазифаларни бажара олади:

- бошқарилувчи компьютер ва қурилмалардаги бузилишларни кузатиш, сабабларни аниқлаш ва бартараф этиш (кўпинча автоматик тарзда), оқибатларини тузатиш ва бузилишларни олдини олиш (масалан ташҳислаш амалини бажариш орқали);

- компьютерларнинг ва тармоқ қурилмаларининг конфигурацияланишини бошқариш (хусусан, инициализациялаш, қайта конфигурациялаш ва тармоқ қурилмалари ва компьютерларни узиб қўйиш);

-фойдаланувчилар ва фойдаланувчилар гуруҳи томонидан тармоқ ресурсларидан фойдаланишни тартибга солиш (масалан, дискли ва бошқа квоталарни тартибга солиш);

- тармоқ қурилмалари ва сервислар унумдорлигини бошқариш (тармоқ қурилмалари ишлатилиши жадаллиги статистикасини ва хатоликлар частотасини йиғиш ва тахлиллаш ҳамда олинган маълумотлар асосида улар унумдорлигини сунъий тарзда ўрнатиш);

- олдиндан белгиланган хавфсизлик сиёсати асосида тармоқ ресурсларидан фойдаланишни назоратлашдан фойдаланиб маълумотлар ҳимоясини бошқариш ва уларни бузишга уринишлардан маъмурни ҳабардор этиш.

Корхона ахборот хавфсизлиги тизими корпоратив тармоқни бошқариш тизимининг энг муҳим компоненти ҳисобланади. Корхона масштабидаги тақсимланган тармоқда ахборотни ҳимоялаш воситаларини бошқарувчи тизим қуйидаги вазифаларни бажариши лозим:

- корхона тармоғи доирасида хавфсизлик сиёсатини бошқариш, алоҳида қурилмалар хавфсизлигининг локал сиёсатини шакллантириш ва уни ахборотни ҳимояловчи барча қурилмаларга етказиш;

- фойдаланиш объектларини ва субъектларини конфигурациялашни бошқариш; ҳимоя қурилмалари ва дастурий таъминоти таркибини, версиясини, компонентларини бошқаришни ўз ичига олади;

- тақсимланган татбиқий тизимларга ҳимоя сервисларини тақдим этиш, ҳимояланган иловалар ва улар ресурсларини руйхатга олиш. Иловаларнинг бу гуруҳи, аввало, татбиқий тизимлар томонидан ҳимоя сервисларини бошқариш учун интерфейсни таъминлаш лозим;

- криптовоситаларни бошқариш, хусусан калитли бошқариш (калитли инфратсруктура). Калитли инфратузилма инфратузилма хизмати таркибида ишлаши лозим;

- ходисавий протоколлаш; турли қурилмаларга *логларни* беришни созлашни, логларни деталлаштириш сатхини бошқаришни, протокол олиб борилувчи ходисаларни таркибини бошқаришни ўз ичига олади;

- ахборот тизими хавфсизлигини аудитлаш; ахборот тизимлари ҳимояланишининг жорий ҳолати хусусидаги объектив маълумотларни баҳолашни таъминлайди;

- тизим хавфсизлигини мониторинглаш; қурилмалар ва қурилмаларда кечувчи ходисалар (ҳимоялаш контексти бўйича) ҳолати, фаоллиги хусусида, масалан, бўлиши мумкин бўлган хужумлар хусусида реал вақтда ахборот олинишини таъминлайди;

- махсус ҳимояланган иловалар, масалан амаллар устидан нотариал назорат ишини таъминлаш ҳамда регламентда кўзда тутилган тадбирларни (калитларни, паролларни, ҳимоя қурилмаларини алмаштириш, смарт-карталарни ишлаб чиқариш ва ҳ.) мададлаш;

- иловаларнинг лойиҳа-инвентаризациялаш гуруҳи ишини таъминлаш. Иловаларнинг бу гуруҳи корхона тармоғига ҳимоя воситаларини ўрнатишни, қўлланиладиган ҳимоя воситаларини ҳисобга олишни, ҳимоя воситаларининг модул таркибини назоратлашни, ҳимоя воситалари ҳолатини назоратлашни ва ҳ. бажаради.

Тармоқларни анъанавий бошқариш тизими ва тармоқдаги ахборотни ҳимоялаш воситаларини бошқариш тизими орасида ўзаро алоқани комплекслаш ва ташкил этиш муаммоси мавжуд.

13.2. Хавфсизлик воситаларини бошқариш архитектураси

Компаниянинг тақсимланган ахборот тизимида ўзининг хавфсизлик сиёсатини муваффақиятли амалга ошириши учун хавфсизликни бошқариш марказлиштирилган бўлиши ва ишлатиладиган операцион тизимга ва татбиқий тизимларга боғлиқ бўлмаслиги лозим. Ундан ташқари, корпора-

тив ахборот тизимида кечувчи жараёнларни (рухсатсиз фойдаланиш, фойдаланувчилар имтиёзини ўзгариши ва ҳ.) рўйхатга олиш тизими ягона бўлиши ва маъмурга корпоратив ахборот тизимидаги барча ўзгаришларнинг тўлиқ кўринишини тасаввур этишига имкон бериши лозим.

Корпоратив ахборот тизими хавфсизлигини марказлаштирилган бошқариш асосида глобал бошқариш концепцияси GSM (Global Security Management) ётади. Ушбу концепция корхона ахборот ресурсларини қуйидаги хусусиятларга эга бўлган комплекс бошқариш тизимини қуришга имкон беради:

- корхонанинг барча ресурслари (хавфсизлик сиёсати объектлари) учун ҳимоялашнинг яхлитлигини, зиддиятлик эмаслигини ва қоидалар тўпламининг тўлалигини таъминловчи, барча мавжуд ҳимоя воситаларини корхона хавфсизлиги сиёсати асосида бошқариш;

- ресурсларни тавсифловчи шахсий воситалар ҳамда корхонанинг бошқа каталоглари билан алоқаси бўйича фаоллашувчи корхона муҳитининг ягона (тақсимланган) каталоги орқали корхонанинг барча ресурсларини аниқлаш;

- хавфсизлик сиёсатига асосланиб, ахборотни ҳимоялашнинг локал воситаларини марказлаштирилган бошқариш;

- корхона муҳитида сиёсат объектларини токенлар ва очиқ калитлар инфратузилмасидан фойдаланиб қатъий аутентификациялаш;

- каталогда белгиланган корхона ресурсларидан ёки бутун каталог қисмларидан фойдаланишни маъмурлашнинг кенгайтирилган имкониятлари;

- ҳисоб-китобликни (корпоратив тармоқ масштабида тизимнинг тақсимланган объектларининг ўзаро алоқасидаги барча амалларини рўйхатга олиш) ва аудитни, хавфсизлик мониторингини, хавотирли сигнализацияни таъминлаш;

- умумий бошқариш тизимлари ва хавфсизликнинг инфратузилма тизимлари билан интеграцияланиши;

Ушбу концепция доирасида "хавфсизлик сиёсатига асосланган PBM (Policy Based Management) бошқариш" деганда корхона бизнес-объекти учун таърифланган қоидалар тўплами тушунилади. Бу қоидалар тўплами

объектларнинг бизнес-соҳани тўлиқ қамраб олишини ва ишлатилувчи бошқариш қоидаларининг зиддиятлик эмаслигини кафолатлайди.

РВМ принципларига асосланган, корхона хавфсизлигини бошқаришга мўлжалланган GSM бошқариш тизими қуйидаги талабларга жавоб беради:

- корхона хавфсизлиги сиёсати мантиқий ва семантик боғланган, шаклланувчи, таҳрирланувчи ва тахлилланувчи маълумотларнинг бир бутун тузилмасидан иборат;

- корхона хавфсизлиги сиёсати ягона контекстда ҳимоянинг барча сатҳлари учун ҳимоянинг тармоқ сиёсати ва корхона ахборот ресурслари хавфсизлик сиёсатининг бир бутуни сифатида белгиланади;

- корхона ресурсларини ва хавфсизлик сиёсатини маъмурлашни енгиллаштириш мақсадида сиёсат параметрлари сони минималлаштирилади.

GSM бошқариш тизими хавфсизлик сиёсатининг корхона хавфсизлиги концепцияси моделига мослигини текширувчи кўп мезонли воситалар эвазига хавфсизлик сиёсатини таҳлиллашнинг турли-туман механизмларини таъминлайди.

Хавфсизликнинг глобал ва локал сиёсатлари

Корхона хавфсизлигининг глобал сиёсати ахборот хавфсизлиги контекстида корпоратив тармоқ объектлари ўзаро алоқасининг параметрларини тавсифловчи хавфсизлик қоидаларининг чекли тўпламидир.

Бунда хавфсизликнинг глобал сиёсати объекти сифатида алоҳида ишчи станциялари ва қисм тармоқлар ҳамда ўз ичига компаниянинг бутун тузилмавий бўлимларини олувчи (масалан, маркетинг бўлими ёки молиявий департамент) объектлар гуруҳи ёки ҳатто алоҳида компания кўрилиши мумкин.

Хавфсизликнинг глобал сиёсати тармоқдаги ўзаро алоқага, ҳамда тизимнинг назоратлаш ва бошқариш функцияларига тааллуқли бўлиши мумкин. Бажарадиган функциялари бўйича хавфсизликнинг глобал сиёсати қуйидаги гуруҳларга бўлинади:

- *VPN қоидалари*. Қоидаларнинг бу гуруҳи IPSec протоколлари ёрдамида амалга оширилади;

- *пакетли фильтрлаш қоидалари.* Бу қоидалар Stateful ва Stattles хилидаги пакетли фильтрлашни таъминлайди.

- *proxy-қоидалар.* Бу қоидалар берилган татбиқий протоколлар бошқарувида узатилувчи трафикни фильтрлашга жавоб беради;

- *аутентификацияланган/авторизацияланган фойдаланиш қоидалари*;

- *сигнализацияга ва ходисавий протоколлашга жавоб берувчи қоидалар*.

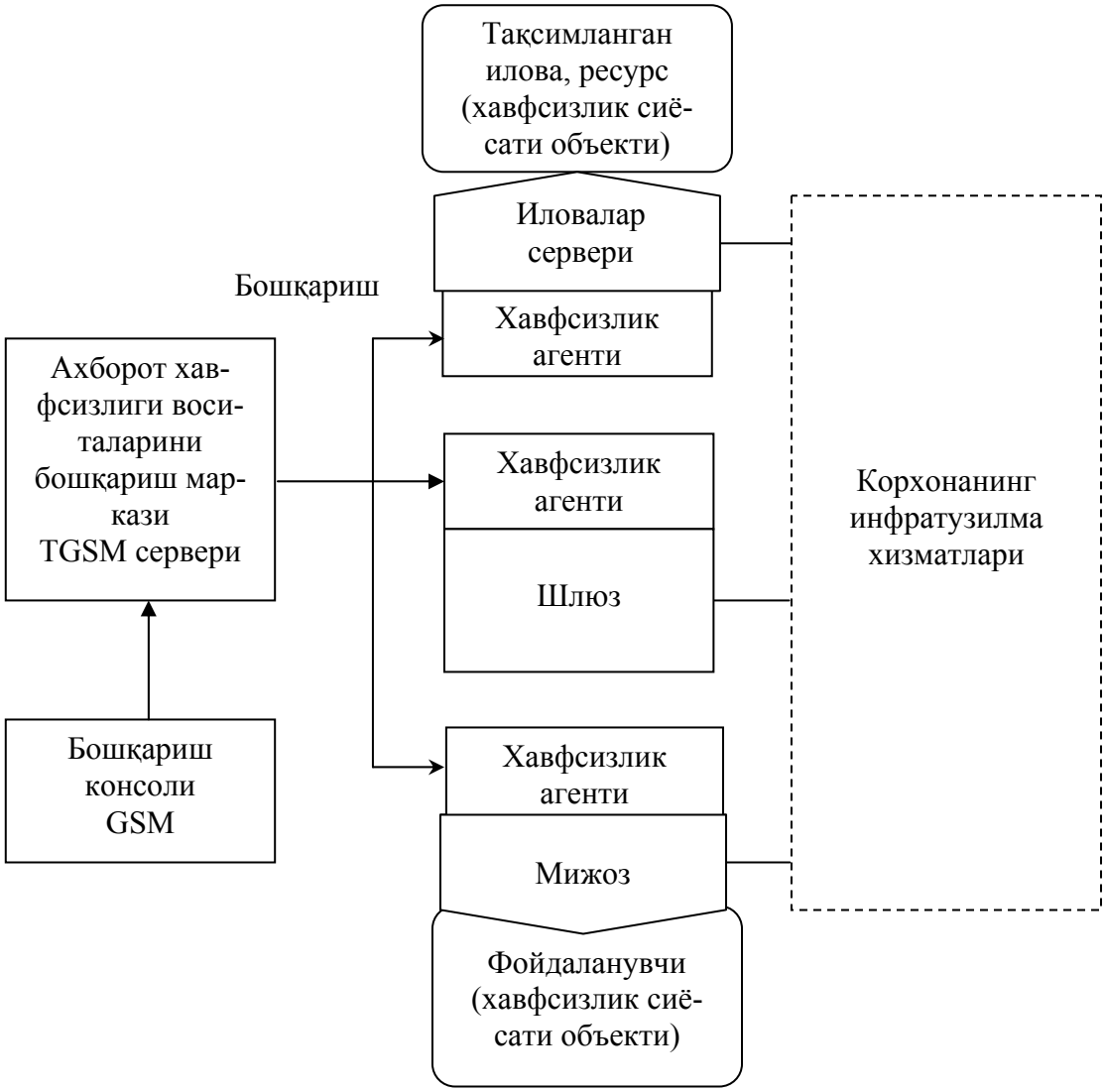
Хавфсизликнинг глобал сиёсати тармоқ сатҳида хавфсизлик сиёсатининг мантиқий яхлит ва семантик тўлиқ тавсифи бўлиб, унинг асосида алоҳида қурилмалар хавфсизлигининг локал сиёсати қурилиши мумкин.

Хавфсизликнинг локал сиёсати ахборот хавфсизлигининг қандайдир сервисини амалга оширувчи ҳар қандай ҳимоялаш воситасига зарур ҳисобланади. Анъанавий ёндашишда маъмурга ҳар бир ҳимоя воситасини алоҳида созлашга ёки энг оддий созлашни узелларнинг катта сонига қайтаришга (репликациялашга) тўғри келар эди. Равшанки, бу маъмурлашнинг катта сонли хатолигига олиб келар ва натижада корпоратив тармоқнинг ҳимояланиш даражаси жиддий пасаяр эди.

Маъмур томонидан хавфсизликнинг глобал сиёсати шакллантирилганидан сўнг бошқариш маркази унинг асосида ҳар бир ҳимоя воситаси учун автоматик тарзда ҳимоялашнинг алоҳида локал сиёсатини ҳисоблайди ва мос ҳимоя воситасининг бошқариш модулига зарурий созлашларни автоматик тарзда юклайди.

Тармоқда хавфсизликнинг глобал сиёсатини ва муайян қурилмада хавфсизликнинг локал сиёсатини амалга ошириш қоидаларининг бир-биридан фарқи шундаки, хавфсизликнинг глобал сиёсатидаги қоидаларда фойдаланиш объектлари ва субъектлари тармоқ чегарасида ихтиёрий равишда тақсимланиши мумкин, хавфсизликнинг локал сиёсатидаги қоидалардан эса фақат тармоқ қурилмаларидан бирининг муҳити чегарасида фойдаланиш мумкин.

Ахборот хавфсизлиги воситаларини бошқариш тизимининг умумий тузилма схемаси 13.4–расмда келтирилган. Асосий хавфсизлик воситаларининг вазифалари қуйидагича. Мижоз шахсий компьютерида ўрнатилган *хавфсизлик агенти* одатда "мижоз-сервер" иловаларида мижоз сифатида



13.4–расм. Ахборот хавфсизлиги воситаларини бошқариш тизимининг умумий тузилма схемаси

қатнашувчи алоҳида фойдаланувчини ҳимоялашга мўлжалланган.

Иловалар серверига ўрнатилган *хавфсизлик агенти* тақсимланган иловаларнинг сервер компоненти хавфсизлигини таъминлашга мўлжалланган. Шлюз компьютерига ўрнатилган *хавфсизлик агенти* турли тармоқ хавфсизлиги сиёсатини мувофиқлаштириш масаласини ечган ҳолда, корхона ичида ёки корхоналар орасида тармоқ агентларини ажратилишини таъминлайди.

Бошқариш маркази тармоқ масштабида хавфсизликнинг глобал сиёсатини тавсифлашни, глобал сиёсатни ҳимоялаш қурилмаси хавфсизлигининг

локал сиёсатига трансляциялашни, ҳимоялаш қурилмасини юклашни ва тизимнинг барча агентлари ҳолатини назоратлашни таъминлайди.

Бошқариш консоли маъмур (маъмурлар) иш жойини ташкил этишга мўлжалланган. GSMнинг ҳар бир сервери учун бир неча консоллар ўрнатилиши мумкин.

Хавфсизликнинг локал агенти охирги қурилмада (мижозда, серверда, шлюзда) жойлаштирилувчи дастур бўлиб, қуйидаги функцияларни бажаради:

- хавфсизлик сиёсати объектларини аутентификациялаш, жумладан аутентификациялашнинг турли сервисларини интеграциялаш;
- тизимдаги фойдаланувчини ва у билан боғлиқ ходисаларни аниқлаш;
- хавфсизлик воситаларини марказлаштирилган бошқаришни ва фойдаланиш назоратини таъминлаш;
- иловалар манфаати учун ресурсларни бошқариш, татбиқий сатҳ ресурсларидан фойдаланишни бошқаришни мададлаш;
- трафикни ҳимоялаш ва аутентификациялаш;
- трафикни фильтрлаш;
- ходисавий протоколлаш, мониторинг, хавотирли сигнализация.

Локал агентнинг марказий элементи – хавфсизликнинг локал сиёсатининг процессори (LSP processor) хавфсизликнинг локал сиёсатини изоҳлайди ва бошқа компонентлар орасида чақиришларни тақсимлайди.

13.3. Ахборот тизимларининг аудити ва мониторинги

Ахборот хавфсизлиги тизими амалга оширилганида тармоқ инфратузилмасини мураккаблиги, маълумотлар ва иловаларнинг турли-туманлиги сабабли кўпгина таҳдидлар хавфсизлик маъмурининг эътиборидан четга қолиши мумкин. Шунинг учун ахборот тизимларининг мунтазам аудити ва доимий мониторинги амалга оширилиши зарур.

Ахборот тизимлари хавфсизлигининг аудити. Аудит-корхонанинг алоҳида соҳаларини мустақил экспертизаси. Корхона аудитининг ташкил этувчиларидан бири унинг ахборот тизими аудити ҳисобланади. Ахборот тизимларининг аудити – ахборот тизимининг ҳимояланишининг жорий ҳолати, ундаги ҳаракатлар ва ходисалар хусусидаги объектив маълумотларни олиш ва баҳолаш, улар сатҳининг белгиланган мезонга мослигини аниқловчи тизимли жараёндир. Аудит ўтказилиши ахборот тизимининг жорий хавфсизлигини баҳолашга, хавф-хатарни баҳолашга, уларнинг ташкилот бизнес-жараёнларига таъсирини баҳоратлашга ва бошқаришга, ташкилот ахборот ресурслари хавфсизлигини таъминлаш масаласига асосли ёндашишга имкон беради.

Ахборот тизимлари хавфсизлигининг аудити қуйидаги босқичларни ўз ичига олади:

- аудит муолажасининг бошланиши;
- аудит ахборотини йиғиш;
- аудит маълумотларини тахлиллаш;
- тавсиялар ишлаб чиқиш;
- ҳисобот тайёрлаш.

Аудит босқичларининг бажарилиш кетма-кетлиги 13.5–расмда келитирилган.

Аудит муолажасининг бошланиши. Аудит, бу масалада манфаатдор ҳисобланувчи, компания раҳбарияти ташаббуси билан ўтказилади. Аудит тадбирларнинг комплекси бўлиб, унда аудитор билан бирга компаниянинг аксарият тузилмавий бўлинмаларининг вакиллари қатнашади. Бу жараёнда иштирок этувчиларининг харакатлари аниқ мувофиқлаштирилиши шарт. Шу сабабли, аудит муолажасининг бошланиши босқичида аудит ўтказиш режасини тайёрлаш ва тасдиқлаш, аудитор хуқуқи ва мажбуриятини белгилаш билан боғлиқ ташкилий масалалар ечилиши лозим.

Аудит муолажасининг бошланиши босқичида текшириш доираси аниқланиши лозим. Компаниянинг ахборот қисми тизимининг бирини конфиденциаллик нуқтаи назаридан аудитга тортиб бўлмаса, иккинчисини,

етарлича жиддий бўлмаганлиги сабабли, аудит доирасидан чиқариш мумкин.

13.5–расм. Аудит босқичларининг бажарилиш кетма-кетлиги.

Аудит ахборотини йиғиш. Бу босқич энг мураккаб ва узоқ давом этади. Бунга сабаб, ахборот тизимга керакли хужжатларнинг йўқлиги ва аудиторнинг ташкилотнинг кўпгина лавозимли шахслари билан бевосита ўзаро мулоқотда бўлиши зарурияти. Аудитор ташкилот, ахборот тизимининг ишлаши ва жорий ҳолати хусусидаги ахборотни компаниянинг жавобгар шахслари билан махсус ташкил этилган сухбат орқали, техникавий ва ташкилий-бошқариш хужжатларни ўрганиш йўли билан, ҳамда ихтисослаштирилган дастурий воситалар ёрдамида ахборот тизимини тадқиқлаш орқали олади.

Аудит маълумотларини тахлиллаш. Тахлиллаш ахборот тизимларининг аудитида энг маъсулиятли босқич ҳисобланади. Тахлиллашда ноаниқ, эскирган маълумотлардан фойдаланиш ножоиздир, шу сабабли маълумотларга аниқлик киритилиши ва ахборотлар жиддий йиғилиши мумкин. Аудит маълумотларини тахлиллашда қуйидаги учта ёндашишдан фойдаланилади.

Биринчи ёндашиш хавф-хатарларни тахлиллашга асосланади. Хавф-хатарларни тахлиллашдан мақсад мавжуд хавф-хатарларни аниқлаш ва улар катталигини баҳолаш (уларга сифатий ва миқдорий баҳо бериш). Ушбу ёндашиш жуда мураккаб бўлиб, кўп меҳнат сарф этилади ва аудиторнинг энг юқори малакасини талаб қилади.

Иккинчи ёндашиш ахборот хавфсизлиги стандартларидан фойдаланишга асосланган. Стандартлар ахборот тизимларининг кенг синфи учун дунё амалиётини умумлаштириш натижасида шаклланган хавфсизлик талабларининг базавий тўпламини белгилайди. Бу ҳолда аудитордан, берилган ахборо тизими учун стандарт талаблари тўпламини тўғри танлаш талаб этилади. Соддалиги ва ишончлилиги туфайли бу ёндашиш амалда кенг қўлланилади. У ресурсларнинг минимал сарфида ахборот тизими хусусида асосланган хулосалар қилишга имкон беради.

Учинчи ёндашиш олдинги икала ёндашишни комбинациялашни кўзда тутади. Ахборот тизимига қуйиладиган хавфсизликнинг базавий талаблари стандарт орқали аниқланса, берилган ахборот тизими ишлашининг хусусиятларини ҳисобга олувчи қўшимча талаблар хавф-хатарларни тахлиллаш асосида шакллантирилади.

Тавсиялар ишлаб чиқиш. Тахлиллаш натижалари тавсиялар ишлаб чиқиш учун асос бўлади. Аудитор тавсиялари муайян ва берилган ахборот тизимига қўлланиладиган, иқтисодий асосланган, исботланган (тахлиллаш натижалари билан қувватланган), ва муҳимлик даражаси бўйича рутбаланган бўлиши шарт. Аудитнинг мунтазам ўтказилиши ахборот тизимининг барқарор ишлашини кафолатлайди. Шунинг учун профессионал аудит натижаларидан бири кейинги текширишларин ўтказиш режа-графигини шакллантиришдан иборат.

Ҳисобот тайёрлаш. Аудитор ҳисоботи аудит ўтказишнинг асосий хужжати ҳисобланади ва унинг сифати аудитор ишининг сифатини характерлайди.

Ҳисобот таркибида аудит ўтказиш мақсадининг тавсифи, текширилувчи ахборот тизимининг характеристикаси, аудит ўтказиш доираси ва ишлатилувчи усуллар бўйича кўрсатма, аудит-маълумотлари тахлилининг

натижаси, бу натижаларни умумлаштирувчи ва ахборот тизими ҳимояланиш сатҳининг стандарт талабларга жавоб бериши бўйича хулосалар ва албатта, мавжуд камчиликларни бартараф этиш ва ҳимоя тизимини такомиллаштириш бўйича тавсиялар бўлиши лозим.

Ахборот тизимлари хавфсизлигининг мониторинги

Ҳозирда тармоқлараро экран, виртуал хусусий тармоқ, рухсатсиз фойдаланишдан ҳимоялаш воситалари каби ҳимоянинг анъанавий воситалари ишончли ва самарали ахборот хавфсизлиги тизимини қуришга зарур бўлсада, етарли эмас. Чунки бу анъанавий воситалар фақат хужумни блокировка қилишга қодир, аммо хужумларни олдини олиш ва оқибатларини аниқлаш имконияти уларда мавжуд эмас.

Ушбу муаммонинг ечими асосланган ёндашиш фаол аудит технологияси ёки хавфсизликни фаол (адаптив) бошқариш технологияси номини олган. Хавфсизликни фаол бошқариш технологияси қуйидаги компонентларни ўз ичига олади:

- ишчи станциялари, серверлар, маълумотлар базасини бошқарувчи тизимлар, тармоқ уланишлари ва Internet ва бошқа глобал тармоқларга уланиш нуқталари каби ахборот тизими объектлари ҳимояланишини тахлилловчи ва заифликларини қидирувчи воситалар;

- хужумларни аниқлаш ва тахлиллаш воситалари;

- инфратузилма ўзгаришида ёки хужумларда ҳимоялаш воситаларини вақтнинг реал режимида созлашларни мослаштириш ва бошқариш воситалари.

Ахборот хавфсизлиги тизими мониторинги вазифаларини ҳимояланишни тахлиллаш ва хужумларни аниқлаш воситалари бажаради. Ҳимояланишни тахлиллаш воситалари ишчи станцияларида ва серверларда, маълумотлар базасида операцион тизим ҳимояси элементларининг созланишини тадқиқлайди. Улар тармоқ топологиясини тадқиқлайди, ҳимояланмаган ёки нотўғри тармоқ уланишларини қидиради, тармоқлараро экранлар созланишини тахлиллайди. Ҳимояланишни тахлиллаш воситаларини, уларнинг ишлаши бўйича хавфсизлик сканерлари деб ҳам юритишади. Тахлиллаш натижасида сканер маъмурга юборилувчи, таркибида

аниқланган заифликлар ва уларни йўқотиш қоидалари бўлган ҳисоботни шакллантиради. Агар сканер таркибида хавфсизлик воситалари созланишини бошқарувчи воситалар бўлса, у мустақил тарзда уларни қайта конфигурациялаши мумкин.

Ташкилотнинг замонавий инфратузилмасини ҳисобга олган ҳолда айтиш мумкинки, бундай сканерларнинг мавжудлиги ахборот тизимлари хавфсизлиги мониторингининг муҳим элементи ҳисобланади. Таъкидлаш лозимки, бу воситалар ҳимояни хужум содир бўлишидан аввал амалга оширади.

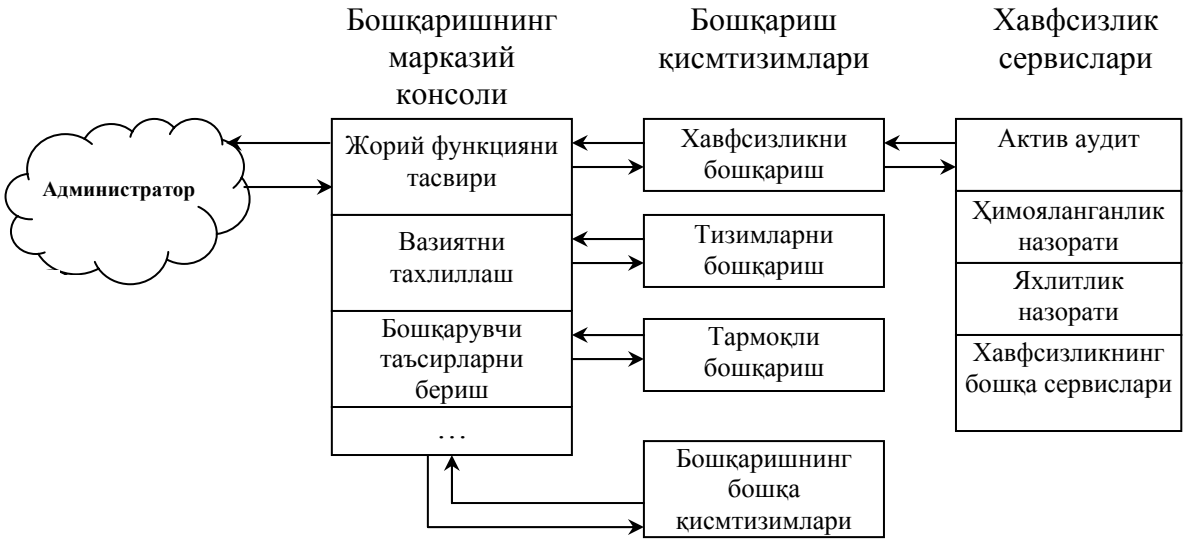
Ахборот тизими хавфсизлиги мониторингининг яна бир зарур элементи хужумларни аниқловчи воситалардир. Хужумларни аниқлаш корпоратив тармоқда кечувчи шубҳали ҳаракатларни баҳолаш жараёнидир. Хужумларни аниқлаш вақтнинг реал режимида тармоқ трафигини, ҳамда операцион тизим ва иловаларнинг руйхатга олиш журналларини тахлиллаш орқали амалга оширилади. Хужумларни аниқлаш тизимининг компонентлари агентлар деб аталади, ва ишчи станцияларда, серверларда жойлаштирилади ёки тармоқнинг қандайдир сегментини ёки бутун тармоқни қоплайди. Агентлар ўзларининг ишида сканерлар каби маълум заифликлар руйхатидан фойдаланиб, ходисаларни ушбу заифликлар билан таққослайди. Қандайдир узелда шубҳали фаолият аниқланганида хужумларни аниқлаш тизими ушбу фаолият фаоллиги хусусидаги огоҳлантиришни маъмурга жўнатади. У огоҳлантиришни узелнинг ўзига жўнатиши ёки узел ишини блокировка қилиш мумкин. Ушбу тизимнинг фарқли хусусияти - унинг бўлиб ўтган хужумларни аниқлаш учун ходисалар журналини тахлиллашидир.

Хавфсизлик воситаларини бошқариш шакли бўйича пассив ва фаол (актив) бўлиши мумкин. Пассив бошқаришда тармоқни бошқариш тизимига ёки маъмурга фақат хабар берилса, фаол бошқаришда хужумловчи узел ёки фойдаланувчи билан мустақил тарзда сессия тугалланади.

Бундан ташқари, бу тизимнинг вазифасига тармоқдаги, иловалардаги ёки ташкилот ахборот тизимининг бошқа компонентларидаги заифликларни йўкотиш бўйича маъмурга тавсиялар ишлаб чиқиш киради.

Фаол аудит тизими (мониторинги) ва умумий бошқариш ўртасида ўзаро алоқани ташкил этиш муҳим масалалардан ҳисобланади. Фаол аудит намунавий бошқариш функцияларини, яъни ахборот тизимдаги фаоллик хусусидаги маълумотларни тахлиллашни, жорий вазиятни акслантиришни, шубҳали фаолликка автоматик тарзда реакция кўрсатилишини бажаради. Тармоқни бошқариш тизими худди шунга ўхшаш ишлайди. Фаол аудит ва умумий бошқаришни умумий дастурий-техник ва ташкилий ечимлардан фойдаланиб интеграциялаш мақсадга мувофиқ ҳисобланади. Бу интеграция-ланган тизимга яхлитликни назоратлаш, ҳамда ахборот тизими ҳатти-ҳаракатларининг ўзига хос жиҳатларини кузатувчи бошқа йўналишдаги агентлар ҳам киритилиши мумкин (13.6-расм).

Бошқаришнинг марказий консоли мавжуд бўлиб, унда фаол аудит (мониторинг) яхлитликни назоратлаш, бошқа жиҳатлар бўйича тизим ва тармоқларни назоратлаш тизимларидан маълумотлар тўпланади. Бу консол-да жорий вазият акслантирилади, ундан автоматик тарзда ёки қўлда бошқариш командалари берилади. Техник ёки ташкилий сабабларга кўра бу консол бир неча ишчи жойи кўринишида физик амалга оширилиши мумкин (хавфсизлик маъмурига жой ажратиш билан).



13.6–расм. Хавфсизлик сервислари ва бошқариш тизимининг интеграцияси.

Тармоқ хавфсизлигини адаптив бошқариш моделидан фойдаланиш барча таҳдидларни назоратлаш ва уларга ўз вақтида реакция кўрсатиш, нафақат таҳдидларни амалга оширишга шароит яратувчи заифликларни

йўқотиш, балки заифликларни пайдо бўлиш шароитларини тахлиллаш имконини беради.

13.4. Хавф-хатарларни тахлиллаш ва бошқариш

Хавф-хатарларни тахлиллаш ва бошқариш ахборот тизимидаги таҳдидлар, заифликлар ва хавф-хатарларни баҳолаш, ҳамда ушбу ахборот тизими хавфсизлигининг етарли даражасини таъминловчи қарши чораларни аниқлаш учун ишлатилади.

Хавф-хатарларни тахлиллаш-таҳдидларни, заифликларни ва корпоратив ахборот тизими хавфсизлигига бўлиши мумкин бўлган зарарларни аниқлаш жараёни. Хавф-хатарларни тахлиллашдан мақсад мавжуд хавф-хатарларни аниқлаш ва улар меъёрини баҳолаш (уларга миқдорий баҳо бериш). Хавф-хатарларни тахлиллаш компьютер ахборот тизими хавфсизлигини текшириш бўйича тадбирни ўз ичига олади. Бу тадбирга биноан қайси ресурсларни қайси таҳдидлардан ҳимоялаш зарурлиги ҳамда у ёки бу ресурслар қандай даражада ҳимояга муҳтож эканлиги аниқланади.

Хавф-хатарларни тахлиллашга турли ёндашишлар мавжуд. Ёндашишни танлаш ташкилотда ахборот хавфсизлиги режимига қуйиладиган талаблар даражасига ва эътиборга олинувчи таҳдидлар характерига (таҳдидлар таъсири спектрига) боғлиқ. Талабларнинг иккита даражаси фарқланади:

- ахборот хавфсизлиги режимига минимал талаблар;
- ахборот хавфсизлиги режимига оширилган талаблар.

Ахборот хавфсизлиги режимига минимал талаблар *ахборот хавфсизлигининг базавий даражасига* мос келади. Бу даражадан, одатда, намунавий лойиҳа ечимларида фойдаланилади. Хавф-хатарларни тахлиллаш соддалаштирилган схема бўйича ўтказилади: хавфсизликка таҳдидларнинг кўп тарқалган тўплами уларнинг эҳтимоллигини баҳоламасдан кўрилади. Вируслар, асбоб-ускуналарнинг бузилиши, рухсатсиз фойдаланиш ва ҳ. каби эҳтимоллиги юқори таҳдидларнинг минимал тўплами кўриладиган қатор стандартлар ва спецификациялар мавжуд. Бундай таҳдидларни бетарафлаштириш учун уларнинг амалга оширилиши эҳтимоллиги ва, ресурсларнинг заифлигидан қатъий назар, қарши чоралар кўрилиши лозим, яъни базавий даражада таҳдидлар характеристикаларини кўриш шарт эмас.

Ахборот хавфсизлиги режимига оширилган талаблар, ахборот хавфсизлиги режимининг бузилиши оғир оқибатларга сабаб бўлганида ва ахборот хавфсизлиги режимига минимал талаблар етарли бўлмаганида ишлатилади.

Ахборот хавфсизлиги режимига оширилган талабларни таърифлаш учун ресурслар аҳамиятини аниқлаш, тадқиқланувчи ахборот тизими учун долзарб бўлган таҳдидлар руйхати билан стандарт тўпламни тўлдириш, таҳдидлар эҳтимоллигини баҳолаш ва ресурслар заифлигини аниқлаш зарур.

Хавф-хатарни тахлиллаш жараёнини қуйидаги босқичларга ажратиш мумкин:

- корпоратив ахборот тизимининг таянч ресурсларини идентификациялаш;

- у ёки бу ресурснинг муҳимлигини аниқлаш;

- таҳдидларнинг амалга оширилишига имкон берувчи мавжуд хавфсизлик таҳдидларни ва заифликларни идентификациялаш;

- хавфсизликка таҳдидларни амалга оширилиши билан боғлиқ хавф-хатарларни ҳисоблаш.

Ресурслар учта категорияга – ахборот ресурсларига, дастурий таъминотга ва техник воситаларга (файл серверлари, ишчи станциялар, кўприқлар, маршрутизаторлар ва ҳ.) бўлинади. Ҳар бир категория ичида ресурсларни синфларга ва қисм синфларга ажратиш мумкин. Фақат корпоратив ахборот тизими функционаллигини белгиловчи ва хавфсизликни таъминлаш нуқтаи назаридан муҳим бўлган ресурлар идентификацияланиши лозим.

Ресурснинг муҳимлиги (нарҳи) бу ресурснинг конфиденциаллиги, яхлитлиги ёки фойдаланувчанлиги бузилганида етказилган зарар миқдори билан белгиланади. Ресурслар нархини баҳолашда ресурсларининг ҳар бир категорияси учун бўлиши мумкин бўлган зарар миқдори белгиланади.

Намунавий хавфсизлик таҳдидларига корпоратив ахборот тизими ресурсларига локал масофадан хужумлар, табиий офат, ходимлар хатоси, дастурий таъминотдаги хатолик ёки аппаратуранинг носозлиги сабаб бўлувчи

корпоратив ахборот тизим ишидаги бузилишлар тааллуқли. Таҳдид даражаси деганда унинг амалга оширилиши эҳтимоллиги тушунилади.

Ҳимоянинг бўшлиги корпоратив ахборот тизимидаги заифликларга сабаб бўлади. Заифликларни баҳолаш хавфсизлик таҳдидларининг муваффақиятли амалга оширилиш эҳтимоллигини аниқлашни назарда тутади. Шундай қилиб, зарар етказиш эҳтимоллиги таҳдидларнинг амалга оширилиши эҳтимоллиги ва заифлик миқдори орқали аниқланади.

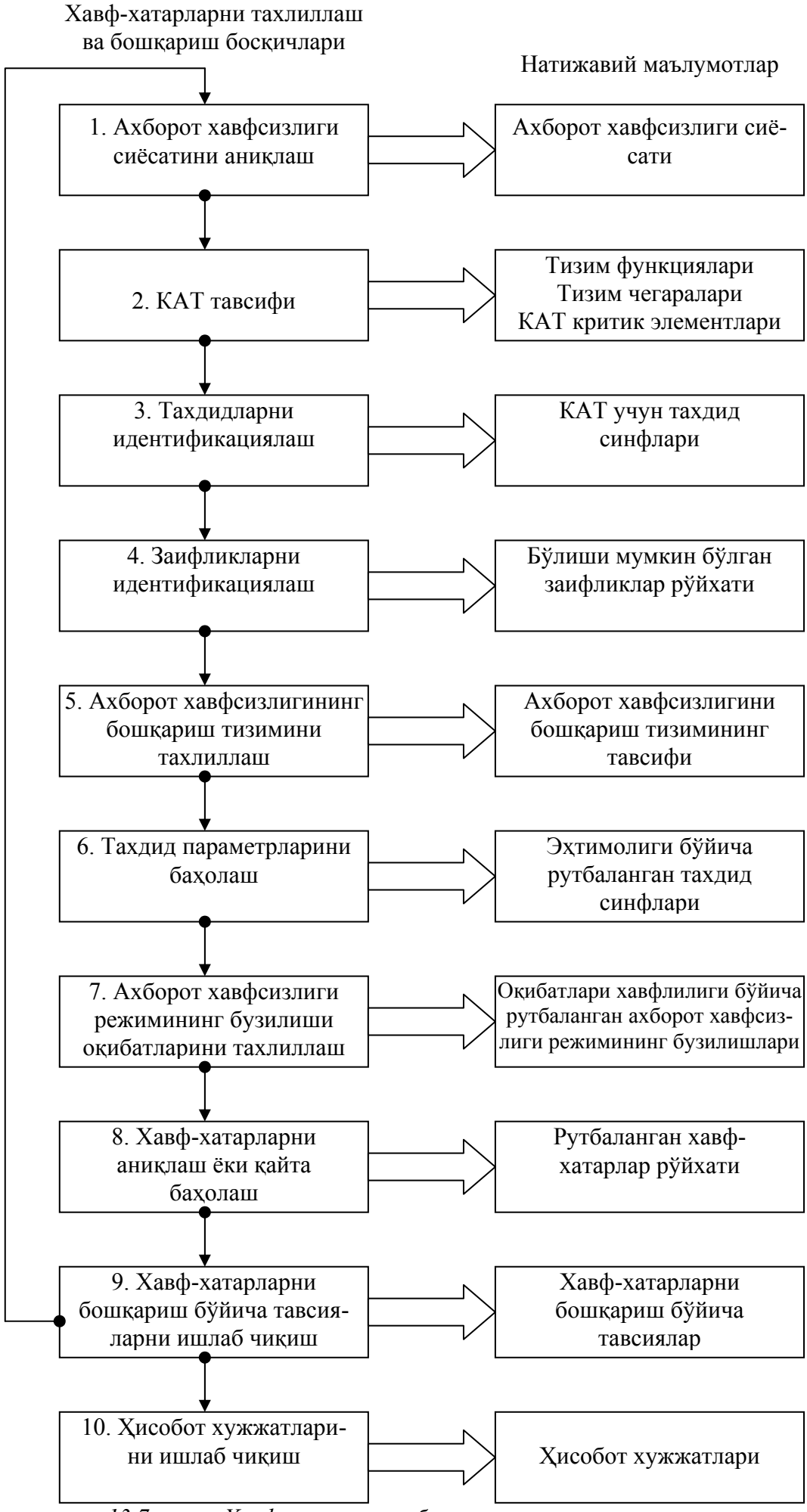
Хавф-хатар даражаси ресурс нархи, таҳдид даражаси ва заифлик миқдори асосида аниқланади. Ресурс нархи, таҳдид даражаси ва заифлик миқдори ошиши билан хавф-хатар даражаси ҳам ошади. Хавф-хатарлар даражасини баҳолаш асосида хавфсизлик талаблари белгиланади.

Хавф-хатарларни бошқариш масаласи, хавф-хатар даражасини мақбул миқдоргача камайтиришга имкон берувчи қарши чораларни асосли танлашни ва амалга ошириш нархини баҳолашни ўз ичига олади. Табиийки, қарши чораларни амалга ошириш нархи бўлиши мумкин бўлган зарар миқдоридан кам бўлиши керак.

13.7-расмда хавф-хатарларни бошқариш технологиясининг босқичлари келтирилган.

Ахборот хавфсизлиги сиёсатини аниқлаш. Бу босқичда ахборот хавфсизлиги соҳасидаги қўлланма-хужжатлар, стандартлар, ахборот хавфсизлигининг асосий қоидалари, хавф-хатарларни бошқаришга ёндашишлар аниқланади ҳамда қарши чоралар структуризацияланади ва корпоратив ахборот тизимини сертификациялаш тартиби белгиланади.

Корпоратив ахборот тизимини (КАТ) тавсифлаш. Ушбу босқичда ахборот хавфсизлиги соҳасидаги ҳалқаро, давлат ва корпоратив стандартларга биноан корпоратив ахборот тизимнинг функционал вазифалари тавсифланади. Компаниянинг критик ахборот ресурслари, жараёнлари ва сервислари тавсифланади; корпоратив ахборот тизимининг чегаралари ҳамда бошқариш ва маълумотлар бўйича энг муҳим компонентларининг таркиби ва боғланишлари аниқланади.



13.7–расм. Хавф-хатарларни бошқариш технологиясининг варианти.

Таҳдидларни идентификациялаш. Ушбу босқичда таҳдидлар руйхати тузилади ва уларнинг даражаси баҳоланади. Бунда турли ташкилотларнинг таҳдидлар синфлари рўйхатидан ҳам берилган таҳдидни амалга ошириш эҳтимоллигининг рейтинги ёки ўртача қийматидан фойдаланиш мумкин.

Заифликларни идентификациялаш. Ушбу босқичда берилган корпоратив ахборот тизимининг заифликлари рўйхати, уларнинг амалга оширилишидаги жоиз натижалар кўрсатилган ҳолда тузилади. Мавжуд корпоратив ахборот тизими учун рўйхатлар қатор манбалардан фойдаланилиб тузилади. Бу манбаларга заифликларни тармоқ сканерлари, турли ташкилотларнинг заифликлар каталоги, хавф-хатарларни тахлилловчи ихтисослаштирилган усуллар киради.

Корпоратив ахборот тизимининг бошқариш тизимини тахлиллаш. Ушбу босқичда бошқариш, тизими, аниқланган таҳдидларга ва заифликларга жоиз бўлган таъсир нуқтаи назаридан тахлилланади.

Таҳдидлар параметрларини баҳолаш. Ушбу босқичда ходисага олиб келувчи заифликнинг амалга оширилиши имконияти баҳоланади. Баҳолашнинг намунавий шкаласи – бир неча рутбали (масалан, паст, ўрта, ва юқори сатҳ) сифатий (балли) шкаладир. Бундай баҳо эксперт томонидан мавжуд объектив факторларни ҳисобга олган ҳолда берилади.

Ахборот хавфсизлиги режимининг бузилиши оқибатларини тахлиллаш. Ушбу босқичда ахборот хавфсизлиги режимининг бузилиши баҳоси аниқланади. Бузилиш оқибатлари молиявий йўқотишларга, обрўсизланишга, расмий тузилмалар томонидан кўнгилсизликларга ва ҳ. сабаб бўлиши мумкин. Бузилиш оқибатларини баҳолаш учун мезонлар тизими танланади ва оқибатлар оғирлигини баҳолаш учун интеграцияланган шкала белгиланади.

Хавф-хатарларни баҳолаш. Ушбу босқичда ахборот ресурслари хавфсизлигининг бузилиши хавф-хатар даражаси баҳоланади. Хавф-хатар даражаси қиймати таҳдидлар, заифликлар даражасига ва бўлиши мумкин бўлган оқибатлар оғирлигига боғлиқ. Хавф-хатарларни баҳолашда сифатий ва миқдорий усуллардан фойдаланилади. Сифатий усул ишлатилганда ахборот хавфсизлиги бузилишининг бўлиши мумкин бўлган хавф-хатарлар хавфлилиги даражаси бўйича рутбаланиши лозим. Миқдорий усул ишлатилганда хавф-хатарлар миқдорий шкалаларда баҳоланиши мумкин. Бу тавсия

этилаётган қарши чораларнинг нархи/самарадорлигини тахлиллашни осонлаштиради. Аммо бу ҳолда дастлабки маълумотларни ўлчаш шкалаларига ва ишлатилаётган моделнинг адекватлигига жуда юқори талаблар қуйилади. Оддий ҳолда хавф-хатарни баҳолашда иккита омил-ходиса эхтимоллиги ва бўлиши мумкин бўлган оқибатлар оғирлиги ишлатилиши мумкин.

Хавф-хатарларни бошқариш бўйича тавсияларни ишлаб чиқиш. Ушбу босқичда турли сатҳлар (ташкилий, дастурий-техник) ва хавфсизликнинг алоҳида жиҳатлари бўйича структуризацияланган қарши чораларнинг комплекси тавсия этилиши лозим. Таклиф этилувчи қарши чоралар комплекси хавф-хатарларни бошқаришнинг танланган стратегиясига биноан қурилади.

Ҳисобот хужжатларни ишлаб чиқиш. Ушбу босқичда хавф-хатарларни тахлиллаш ва бошқаришнинг барча босқичлари бўйича иш натижалари акслантирилган ҳисобот хужжатлари тайёрланади.

Таъкидлаш лозимки, ҳозирда ахборот хавф-хатарларини баҳолашни автоматлаштириш мақсадида дастурий маҳсулотлар ишлаб чиқилган.

13.5. Ахборот хавфсизлиги тизимини қуриш методологияси

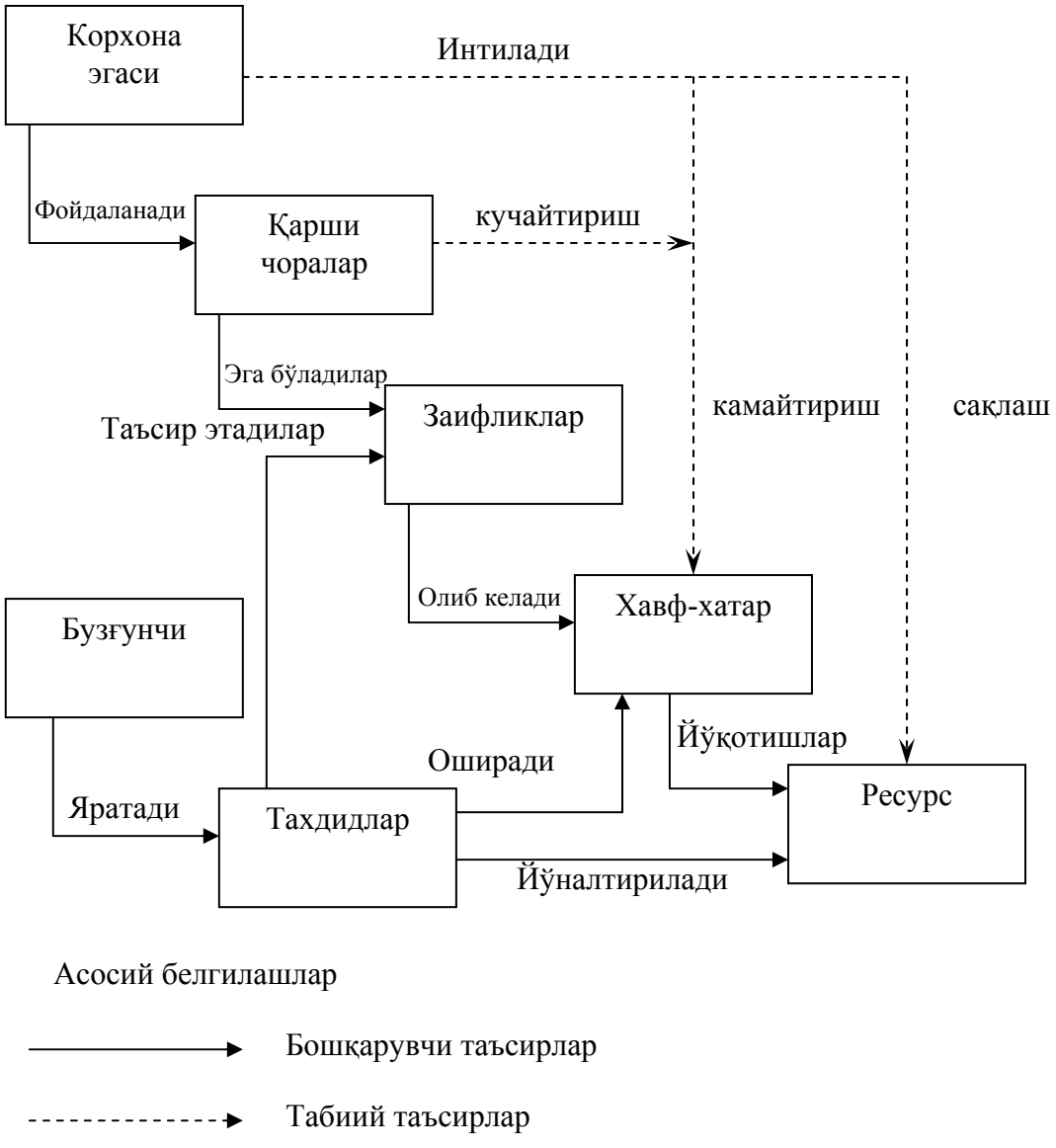
Ахборот хавфсизлиги моделини қуриш. Корхонадаги ахборот хавфсизлиги бўйича тадбирлар қонун чиқариш, ташкилий ва дастурий-техник характерга эга бўлган қатор жиҳатларни қамраб олади. Уларнинг ҳар бирида корхона ахборот хавфсизлигини таъминлаш учун бажарилиши зарур бўлган қатор масалалар таърифланади. Масалаларни ҳал этишда ахборот хавфсизлиги соҳасидаги халқаро стандартларга асосланган корхона ахборот хавфсизлигининг концептуал моделидан фойдаланиш мумкин.

Қуйидаги халқаро стандартлар корпоратив ахборот тизими ҳимояланишини баҳолаш мезонини ва ҳимоялаш механизмларига қуйиладиган талабларни аниқловчи энг муҳим меъёрий хужжатлар ҳисобланади:

- ахборот технологиялари хавфсизлигини баҳолашнинг умумий мезонлари ISO/IEC 15408 (The Common Criteria For Information Technology Security Evalution);

- ахборот хавфсизлигини бошқаришнинг амалий қоидалари ISO/IEC 17799 (Code of practice for Information Security Management).

Ушбу халқаро стандартларга тўла мос равишда тузилган корхона ахборот хавфсизлигининг концептуал модели 13.8-расмда келтирилган.



13.8–расм. Корхона ахборот хавфсизлиги тизимининг концептуаль модели.

Корхона ахборот хавфсизлигининг концептуал моделида қуйидаги омиллар ҳисобга олинган:

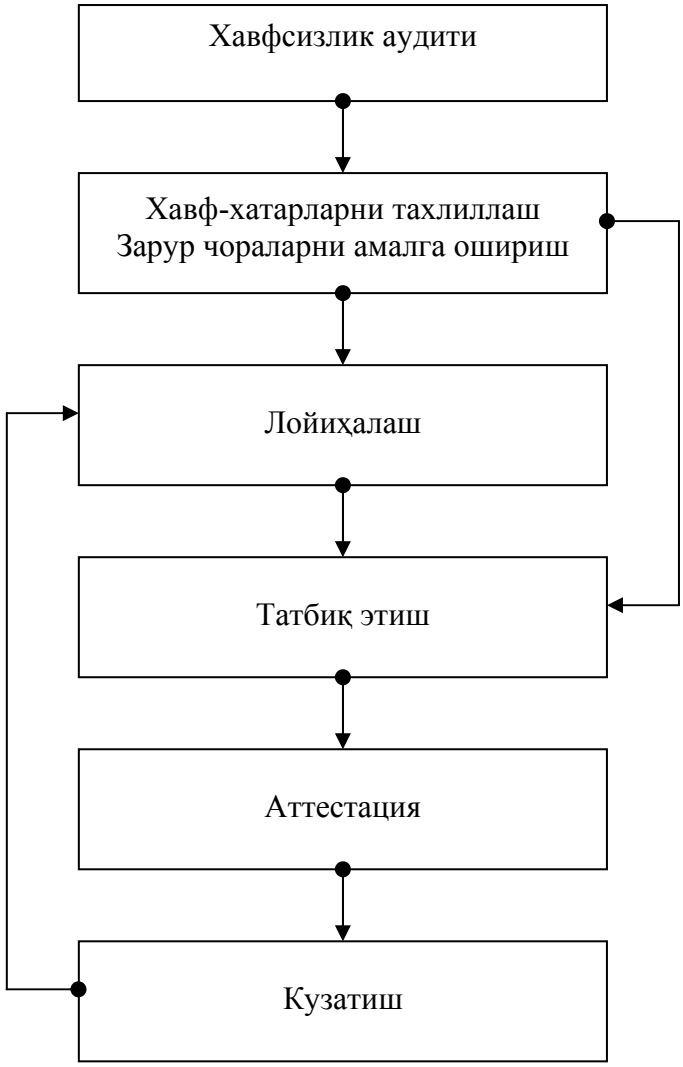
- пайдо бўлиш эҳтимоллиги ва амалга оширилиш эҳтимолиги билан характерланувчи ахборот хавфсизлиги *таҳдидлари*;

- таҳдидларнинг амалга оширилиши эҳтимоллигига таъсир этувчи ахборот тизими ёки қарши чора тизими (ахборот хавфсизлиги тизими) *заифликлари*;

- ахборот хавфсизлигига таҳдидлар амалга оширилиши натижасида корхонага етказилувчи зарарни акслантирувчи омил-*хавф-хатар*.

Бу моделнинг харакатдаги субъектлари – Бузғунчи (таҳдидлар манбаини ифодаловчи) ва Эга (корхона маъмури) объект-Ресурсга қарама-қарши мақсадларда таъсир қиладилар. Ресурс-корхонанинг моддий ва ахборот ресурсларини ва ахборот хавфсизлиги ҳолатини ифодалайди.

Ахборот хавфсизлиги тизимини қуриш босқичлари. Ахборот хавфсизлиги тизимини қуриш босқичларнинг қуйидаги стандартлаштирилган кетма-кетлигида амалга оширилади: хавфсизлик аудити; хавф-хатарларни тахлиллаш, тизимни лойиҳалаш, жорий этиш, аттестациялаш ва кузатиш (13.9-расм).



13.9–расм. Ахборот хавфсизлиги тизимини қуриш босқичлари

Хавфсизлик аудити. Ҳозирда "хавфсизлик аудити" тушунчаси етарлича кенг талқин этилади. Аудитнинг қуйидаги кўринишлари фарқланади.

- ахборот хавфсизлигини тестли бузиш;

- экспресс-текшириш;
- тизимни аттестациялаш;
- лойиҳагача текшириш.

Ахборот хавфсизлиги тестли бузиш корпоратив ахборот тизимининг ҳимояланиш даражасини аниқлаш нуқтаи назаридан самарали ҳисобланмайди. "Бузувчи"нинг асосий мақсади бир икки заифликларни топиб, уларни тизимдан фойдаланишда ишлатиш. Агар "тестли бузиш" муваффақиятли чиқса, ушбу муайян "бузиш"нинг мумкин бўлган сценарийси ривожини олдини олиб, заифликларни қидиришда давом этиш керак. "Тестли бузиш"нинг муваффақиятсизлигини баббаравар тестланувчи тизимнинг ҳимояланганлиги ва тестларнинг етишмаслиги каби талқин қилиш мумкин.

Эксперсс-текшириш доирасида, одатда, кўп вақт сарфини талаб этмайдиган, стандартизацияланган текширишлар асосида корпоратив ахборот тизими хавфсизлик воситаларининг умумий ҳолати баҳоланади. Экспресс-текшириш одатда ахборот ресурсларининг минимал ҳимояланиш даражасини таъминловчи устивор йўналишларни аниқлаш зарурияти туғилганда ўтказилади.

Тизимни аттестациялаш тизимнинг ахборот ресурсларининг ҳимояланиш талабларига мослигини текшириш мақсадида амалга оширилида. Бунда ҳам ташкилий, ҳам техник жиҳатдан талаблар тўплами расмий текширилади, хавфсизлик воситаларининг амалга оширилишининг тўлиқлиги ва етарлилиги кўрилади.

Лойиҳагача текшириш аудитнинг энг кўп меҳнат талаб қиладиган варианти ҳисобланади. Бундай аудит ахборот ресурслари иловаларида корхона ташкилий тузилмасини ва ходимларнинг у ёки бу иловалардан фойдаланиш қоидаларини тахлил этишни кўзда тутади. Сўнгра иловаларнинг ўзи тахлилланади. Ундан кейин бир сатҳдан иккинчи сатҳнинг фойдаланишдаги муайян хизматлар ҳамда ахборот алмашишга зарур бўлган хизматлар тахлилланиши лозим. Сўнгра хавфсизликнинг ўрнатилган воситаларини тахлиллаш билан тасаввур тўлдирилади.

Хавф-хатарларни тахлиллаш 13.4-бўлимда батафсил кўрилган. Ахборот хавфсизлиги бузилганда лойиҳагача текшириш, хавф-хатарларни тахлиллаш билан биргаликда ахборот тизимидаги мавжуд хавф-хатарларни рутбалашга ва адэкват чораларни ишлаб чиқишга имкон беради.

Тизимни лойиҳалаш. Ҳимояни ташкил этиш стратегияси нуқтаи назаридан ресурсли ва сервисли ёндашиш фарқланади. Ресурсли ёндашишда тизим ресурслар тўплами сифатида кўрилади ва ахборот хавфсизлиги тизимининг компонентлари бу ресурсларга боғланади. Ресурсли ёндашиш амалга оширилганида ахборотни ҳимоялаш масаласи хизматлар тузилмасига қўшимча чеклашларсиз ечилади. Бу эса бир жинсли бўлмаган тизим шароитида мумкин эмас. Сервисли ёндашишда тизим фойдаланувчиларга тақдим этилувчи хизматлар тўплами каби талқин қилинади. Ҳозирги вақтда сервисли ёндашиш афзалроқ ҳисобланади, чунки у тизимда амалга оширилган хизматларга боғланади ва "ортиқча" хизматларни рад этиш ҳисобига қатор таҳдидларни истисно қилинишига имкон беради. Бу эса тизимни янада мантиқан асосланган тизимга айлантиради. Айнан сервис ёндашиш хавфсизликнинг замонавий стандартлари, хусусан ISO/IEC 15408 асосида ётади.

Ахборот хавфсизлиги тизимни қуришнинг иккита асосий сценарийси мавжуд: маҳсулотли ва лойиҳали. Маҳсулотли сценарий (ёндашиш) доирасида аввал ҳимоя воситалари тўплами танланади, уларнинг функциялари тахлилланади, сўнгра функциялар тахлили асосида ахборот ресурсларидан фойдаланиш сиёсати белгиланади.

Лойихага харажатлар нуқтаи назаридан махсулотли сценарий энг арзон ҳисобланади. Ундан ташқари, ечимларнинг танқислиги шароитида кўпинча маҳсулотли ёндашиш ягона ҳисобланади (масалан, криптографик ҳимояда фақат шу ёндашиш қўлланилади).

Лойиҳали сценарийда аввал хавфсизлик сиёсати ишлаб чиқилади, унинг асосида хавфсизлик сиёсатини амалга оширишда зарур бўлган функциялар аниқланади, сўнгра бу функциялар бажарилишини таъминловчи ҳимоя воситалари танланади.

Лойиҳали сценарий асосида қурилган тизимлар яхшироқ оптимизацияланган ва аттестациянинг юқори натижаларини беради. Ушбу ёндашиш маҳсулотли ёндашишдан фарқли равишда бошидан у ёки бу платформа билан боғланмаганлиги туфайли, катта гетероген тизимларни қуришда афзал ҳисобланади. Ундан ташқари, узоқ муддатга мўлжалланган ечимларни таъминлайди, чунки хавфсизлик сиёсатини ўзгартирмасдан ечимларни ва ҳимоя воситаларини алмаштиришга имкон беради.

Ахборот хавфсизлиги тизими архитектурасини танлаш нуқтаи назаридан объектли, татбиқий ёки аралаш ёндашишдан фойдаланилади. Объектли ёндашиш ахборот хавфсизлигини у ёки бу объект (бўлинма, филиал, ташкилот) тузилмаси асосида яратади. Объектли ёндашишнинг қўлланиши ташкилий чораларнинг бир жинсли тўпламини мададловчи хавфсизлик механизмлари учун универсал ечимлар тўпламидан фойдаланишни кўзда тутади. Бундай ёндашишга мисол тариқасида ташқи ахборот алмашиш, локал тармоқ, телекоммуникация тизимларининг ва ҳ. ҳимояланган инфратузилмаларини қуришни кўрсатиш мумкин. Объектли ёндашишнинг камчилиги унинг универсал механизмларининг, айниқса, ўзаро мураккаб боғланишли катта сонли иловаларга эга бўлган ташкилотлар учун тугал эмаслиги.

Татбиқий ёндашиш хавфсизлик механизмини муайян иловага боғлаб яратади. Татбиқий ёндашишга мисол тариқасида автоматлаштиришнинг алоҳида масаласи (бухгалтерия, кадрлар ва ҳ.) учун қисм тизимларнинг ҳимоясини кўрсатиш мумкин. Ушбу ёндашишнинг камчилиги – маъмурлаш ва ишлатиш харажатларини минималлаштириш мақсадида хавфсизликнинг турли воситаларини уйғунлаштириш зарурияти.

Аралаш ёндашиш юқорида тавсифланган иккита ёндашишни комбинациялашни кўзда тутади. Бундай ёндашиш лойиҳалаш босқичида кўпроқ меҳнат талаб қилсада, ахборот хавфсизлиги тизимини жорий этиш ва ишлатиш нарҳи бўйича афзалликларни бериши мумкин.

Жорий этиш. Жорий этиш босқичи қуйидаги кетма-кет ўтказилувчи тадбирларни ўз ичига олади:

- ҳимоя воситаларини ўрнатиш ва конфигурациялаш;
- ходимларни ҳимоя воситалари билан ишлашга ўргатиш;

- дастлабки синовни ўтказиш;

- тажрибавий ишлатишга топшириш.

Тажрибавий ишлатиш, ахборот хавфсизлиги тизимини ишчи режимига туширишдан аввал, унинг ишлашидаги мумкин бўлган камчиликларни аниқлашга ва йўқотишга имкон беради. Агар тажрибавий ишлатиш жараёнида компонентларнинг тўғри ишламаслиги фактлари аниқланса, ҳимоя воситалари созланишига ва уларнинг ишлаш режимларига ва ҳ. тузатишлар киритилади.

Тизимни аттестациялаш. Ахборот хавфсизлиги тизимини ваколатли идора томонидан аттестациялаш унинг функционал тўлиқлигини ва корпоратив ахборот тизими ҳимоясининг талаб қилинган даражаси таъминланганлигини тасдиқлашга имкон беради. Тизимнинг аттестацияси хавфсизлик аудитининг бир кўриниши ҳисобланади ва ишлатилувчи чоралар комплекси ва ҳимоя воситаларининг хавфсизлик даражаси талабларига мослигини баҳолаш мақсадида ҳимояланувчи корхонани ишлатишнинг реал шароитларида комплекс текширишни кўзда тутади.

Аттестация натижасида ҳисобот хужжати тайёрланади ва мослик аттестати берилади. Бу аттестат конфиденциал ахборот билан аттестатда кўрсатилган вақт мобайнида ишлаш хуқуқини беради.

Кузатиш. Ахборот хавфсизлиги тизимининг ишга лаёқатлигини ва ўз вазифаларини текис бажарилишини мададлаш учун хавфсизлик тизимининг дастурий ва аппарат таъминотини техник мададлаш ва кузатиш бўйича тадбирлар комплекси кўзда тутилиши лозим. Ахборот хавфсизлиги тизимини техник мададлаш ва кузатиш хизматчи ходимларнинг билими ва кўникмаларини талаб этади ва ҳимояланувчи тизим эгаси – ташкилот штатидаги ахборот хавфсизлигига жавоб берувчи ходимлар томонидан ёки ихтисослаштирилган ташкилот ходимлари томонидан амалга оширилиши мумкин.

Кўрилган методология қоидаларидан фойдаланиш корпоратив ахборот тизимининг умумий ривожи билан бирга ривожлантирилиши ва модификацияланиши мумкин бўлган ахборот хавфсизлигининг самарали ва ишончли тизимини қуришга имкон беради.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. С.С.Қосимов. Ахборот технологиялари. Ўқув қўлланма. – Тошкент. "Алоқачи", 2006.
2. С.К.Ғаниев, М.М. Каримов. Ҳисоблаш системалари ва тармоқларида информация ҳимояси. Олий ўқув юрт.талаб. учун ўқув қўлланма.- Тошкент Давлат техника университети, 2003.
3. В.И. Завгородний. Комплексная защита информации в компьютерных системах: Учебное пособие.-М: Логос; ПБОЮЛ Н.А.Егоров, 2001.
4. Г.Н. Устинов. Основы Информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия "Безопасность".- М.:СИНТЕГ, 2000.
5. Мерит Максим, Девид Поллино. Безопасность беспроводных сетей. Информационные технологии для инженеров.-Москва. 2004.
6. А. Соколов, О. Степанюк. Защита от компьютерного терроризма. Справочное пособие. БХВ-Петербург. Арлит, 2002.
7. А.М. Астахов. Аудит безопасности информационных систем. //Конфидент.-2003.-№1,2.
8. А.В. Беляев. Методы и средства защиты информации // http://www.citforum.ru/internet/infsecure/its2000_01.shtml.
9. Вэк Дж., Карнахан Л. Безопасность корпоративной сети при работе с Интернетом. Введение в межсетевые экраны //Конфидент.-2000.-№4-5.
10. А. Галатенко. Активный аудит//JetInfo.-1999.-№8.
11. А.В. Лукацкий. Адаптивная безопасность сети// Компьютер-Пресс. -1999.-№8.
12. А.В. Лукацкий. Обнаружение атак. – СПб.: БХВ-Петербург, 2001.
13. Р.Норман. Выбираем протокол VPN//Windows2000Magazine.-2001.№7.
14. В.Г. Олифер. Защита информации при работе в Интернет// Connect.-2002. -№11.

15. Н.А. Олифер. Дифференцированная защита трафика средствами IP-Sec //LAN.-2001.-№04; http://www.osp.ru/lan/2001/04/024.htm.
16. Н.А. Олифер. Протоколы IPSec. //LAN.-2001.-№03; http://www.osp.ru/lan/2001/03/024.htm.
17. С.А. Петренко. Построение эффективной системы антивирусной защиты // Конфидент.-2002.-№3.
18. С.А. Петренко. Централизованное управление антивирусной защитой корпоративных сетей Internet/Intranet // Конфидент.-2001.-№2.
19. А.А. Петров. Компьютерная безопасность. Криптографические методы защиты. –М.: ДМК Пресс, 2000.
20. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Уч.пособие для ВУЗов/ Авт.: П.Ю. Белкин и др. –М.:Радио и связь, 1999.
21. Н. Прокофьев. Антивирусная защита сети // Компьютер – Пресс.-2001. –№12.
22. Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. Защита информации в компьютерных системах и сетях: 2-е изд., перераб. и доп. – М.: Радио и связь, 2001.
23. С.В. Симонов. Анализ рисков в информационных системах. Практические советы // Конфидент. -2001. -№2.
24. А.В. Соколов, В.Ф. Шаньгин. Защита информации в распределенных корпоративных сетях и системах. –М.: ДМК Пресс, 2002.
25. Типовые решения по применению средств VPN для защиты информационных ресурсов / ООО "Конфидент". –СПб., 2001.
26. Типовые решения по применению технологии межсетевых экранов для защиты информационных ресурсов / ООО "Конфидент". –СПб., 2001.
27. Типовые решения по применению технологии централизованного управления антивирусной защитой предприятия/ ООО "Конфидент". –СПб., 2002.

28. “Ахборот технологияси. Ахборотларни криптографик мухофазаси. Маълумотларни шифрлаш алгоритми” Ўзбекистон Давлат стандарти. O’zDSt 1105:2006.
29. www.nasa.gov\statistics\
30. www.security.uz
31. www.cert.uz
32. www.uzinfocom.uz

Бошланғич ҳарфлари билан ўқиладиган сўз бирикмалари (қисқартирилган сўзлар)

ACK	Acknowledgement - Тасдиқлаш.
AES	Advanced Encryption Standard - Американинг янги шифрлаш стандарти.
AH	Authentication Header - Аутентификацияловчи сарлавҳа.
ANS	Adaptive Network Security - Хавфсизликни адаптив бошқариш модели
ANSI	American National Standard Institute - АҚШнинг миллий стандартлаштириш институти.
AS	Authentication Server - Аутентифкациялаш сервери
ASA	Adaptive Security Algorithm - Хавфсизликнинг адаптив алгоритми
ASP	Applications Service Providing - Серверда исътемолчидан масофада жойлашган иловаларга Internet ёки хусусий тармоқ орқали хизмат кўрсатиш.
B2B	Business to Business - «бизнес-бизнес» схемаси
B2C	Business to Consumer - «бизнес – истеъмолчи» схемаси
CA	Certification Authorities - Сертификациялаш маркази.
CEK	Content Encryption Key - Маълумотларни шифрлаш калити.
CHAP	Challenge Handshake Authentication Protocol – «Қўл узатиш» муолажаси асосида аутентифкациялаш протоколи
DDoS	Distributed Denial of Service – хизмат кўрсатишдан бош тортишга ундайдиган тақсимланган хужум
DHCP	Dynamic Host Configuration Protocol - Хостларни динамик конфигурациялаш протоколи.
DNS	Domain Name Server - Доменли исмлар хизмати
e business	electronic business - Электрон бизнес.
e commerce	electronic commerce - Электрон тижорат.
ECP	Encryption Control Protocol - Шифрлашни бошқариш протоколи.
ESP	Encapsulated Security Payload - Киритилган узатиладиган ҳимоялаган маълумотлар.
FTP	File Transfer Protocol - Файлларни узатиш протоколи.
GSM	Global System for Mobile Communications - Мобиль алоқанинг глобал тизими.
GSP	Global Security Policy - VPN учун глобал хавфсизлик сиёсати.
HDLC	High level Data Link Control - Юқори сатҳдаги маълумотларни узатиш каналини бошқариш
HMAC	Hashing for Message Authentication - Калитларни хешлаш орқали хабарларни аутентифкациялаш.

HTML HyperText Markup Language - Web-саҳифаларни гиперматнли белгиловчи тил

HTTP HyperText Transfer Protocol - Гиперматнли файлларни узатиш протоколи.

ICMP Internet Control Message Protocol - Internet тармоғида хабарларни бошқариш протоколи.

IETF Internet Engineering Task Force - Internetни лойиҳалаш муаммолари гуруҳи

IKE Internet Key Exchange - Internetда калитларни алмашиш протоколи.

IP Internet Protocol - Тармоқлараро маълумотларни алмашинишнинг Internet протоколи

IPSec Internet Security Protocol - Тармоқлараро маълумотларни хавфсиз алмашиниш Internet протоколи

IRC Internet Relay Chat - Internet да чат-анжуманларни ташкил этиш хизмати

ISO International Standards Organization - Халқаро стандартлаштириш ташкилоти.

ISP Internet Service Provider - Internet хизматларини таъминотчиси

KDC Key Distrubution Center – калитларни тақсимлаш маркази.

KEK Key Encryption Key - Калитларни шифрлаш учун калит

KS Kerberos Server - Kerberos тизими сервери.

L2F Layer2 Forwarding - Иккинчи (канал) сатҳда маълумотларни узатиш протоколи.

L2TP Layer2 Tunneling Protocol - Канал сатҳида маълумотларни туннеллаш протоколи.

LAC L2TP Access Concentrator - L2TP рухсатлар концентратори

LAN Local Access Network - маҳаллий тармоқ.

LCP Link Control Protocol - Уланишларни бошқариш протоколи.

LDAP Lightweight Directory Access Protocol - Каталоглардан фойдаланишларни соддалаштирилган протоколи.

LNS L2TP Network Server - L2TP тармоқ сервери.

LSP Local Security Policy - Маҳаллий хавфсизлик сиёсати (мижоз учун)

MAC Message Authentication Code - Хабарларни аутентификациялаш коди.

MD Message Digest - Хабарлар дайджести

NAT Network Address Translation - Тармоқ адресларини трансляциялаш.

NCP Network Control Protocol - Тармоқни бошқариш протоколи.

NIST National Institute of Standards and Technology - АҚШнинг стандартлар ва технологиялари миллий институти.

NNTP Network News Transfer Protocol - Тармоқ янгиликларини узатиш протоколи

OSI	Open Systems Interconnection - Очиқ тизимлар ўзаро боғлиқлиги
OTK	One Time Key - Бир маротабалик калит.
P2P	Peer to Peer или Partner to Partner - Бизнес муносабатининг «тенг-тенг» схемаси.
PAP	Password Authentication Protocol - Парол бўйича аутентифкациялаш протоколи.
PIN	Personal Identification Number – шахсий идентификация коди
PKD	Public Key Directory - Очиқ калитлар каталоги.
PKI	Public Key Infrastructure - Очиқ калитларни бошқариш инфратузилмаси.
PPP	Point to point Protocol - Икки нуқтали боғланиш протоколи.
PPTP	Point to Point Tunneling Protocol - Икки нуқтали боғланиш учун туннел-лаш протоколи.
POP	Post Office Protocol - фойдаланувчи ўзига келган электрон хабарлардан фойдаланишига имкон берувчи протокол
RADIUS	Remote Authentication Dial In User Service - Фойдаланувчиларни боғланадиган линиялар бўйича масофадан аутентифкациялаш тизими
RAS	Remote Access Service - Масофадан фойдаланаш хизмати
RFC	Request For Comments - Изоҳларни сўрови.
RMON	Remote MONitoring - Тармоқ ускуналарини масофадан мониторинглаш-нинг стандарт спецификацияси.
RSA	Rivest, Shamir, Adleman - Райвест, Шамир, Адлеман. Асимметрик криптоалгоритм.
SHA	Secure Hash Algorithm - Ҳимояланган хешлаш алгоритми
SKIP	Simple Key management for Internet Protocols - Internet протоколи учун калитларни оддий бошқариш.
SMTP	Simple Mail Transfer Protocol - Электрон почтанинг оддий протоколи
SNMP	Simple Network Management Protocol - Тармоқни бошқаришнинг оддий про-токоли.
SPD	Security Policy Database - Хавфсизлик қоидаларининг маълумотлар база-си.
TACACS	Terminal Access Controller Access Control System - Масофадан фойдала-нишни марказлаштирилган назоратлаш протоколи.
TCP	Transport Control Protocol - Узатишларни бошқариш протоколи.
TELNET	Виртуал терминал протоколи – масофадаги компьютерда дастурни бажа-ришга мўлжалланган протокол
TFN	Trible Flood Net – DdoS хужумлар учун инструментал воситалардан бири
TGS	Ticket Granting Server - Мандатларни тарқатиш сервери

TLS	Transport Layer Security - Транспорт сатҳининг ҳимояси.
UDP	User Data Protocol - Фойдаланувчининг маълумотларини узатиш протоколи.
VPN	Virtual Private Network – ҳимояланган виртуал тармоқ.
WAN	Wide Area Network - Глобал тармоқ.
WWW	World Wide Web - Internetнинг гиперматнли ахборотлар хизмати
XML	Extended Mark-up Language – белгилашнинг кенгайтирилган тили
МББТ	Маълумотлар базасини бошқариш тизими